

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2005-226389

(43)Date of publication of application : 25.08.2005

(51)Int.Cl.

E05B 49/00

B60R 25/00

B60R 25/04

(21)Application number : 2004-038022

(71)Applicant : TOKAI RIKA CO LTD  
TOYOTA MOTOR CORP

(22)Date of filing : 16.02.2004

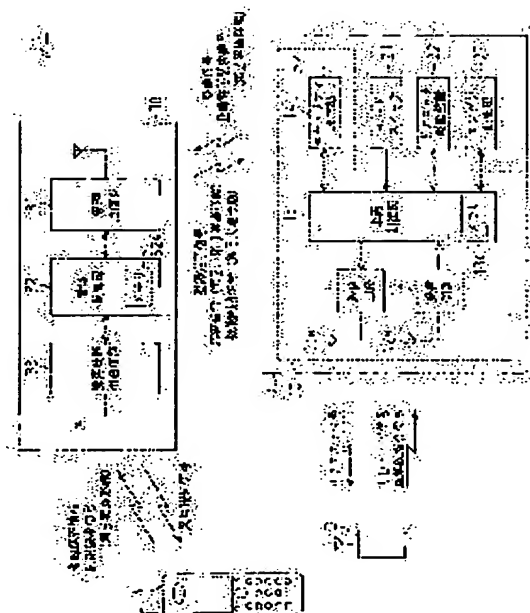
(72)Inventor : KAWAMURA DAISUKE  
OTAKI KIYOKAZU  
YAMAMOTO KEIJI  
SHOMURA KOICHI  
OZAWA TAKAO  
NAKANE YOSHIFUSA

## (54) SECURITY CONTROL SYSTEM, SECURITY CONTROLLER, PORTABLE MACHINE CONTROLLER AND METHOD FOR CONTROLLING SECURITY

## (57)Abstract:

PROBLEM TO BE SOLVED: To provide a security control system, a security controller, a portable machine controller and a method for controlling a security capable of further improving the security level of security apparatus.

SOLUTION: The security controller 10 collates an ID code set to a portable machine 3 and the ID code previously recorded to a memory 13a by a communication with the portable machine 3, and controls a door-lock driving device 22 and an engine control section 23 on the basis of the presence of the organization of the collation. The security controller 10 controls an ID registration, in which the ID code set to the portable machine 3 is recorded to the memory 13a, and transmits a registration signal containing the ID code to be registered to the portable machine controller 30 in the case of the control of the ID registration. The portable machine controller 30 receives the registration signal from the security controller 10, and controls the corresponding portable machine 3 on the basis of the ID code



contained in the registration signal.

\* NOTICES \*

JP0 and INPIT are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.\*\*\*\* shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

---

CLAIMS

---

[Claim(s)]

[Claim 1]

Communication with portable apparatus which has a communication function performs collation with an ID code set as portable apparatus, and an ID code already recorded on an own recording device, It is the security control system provided with a security control device which controls security equipments based on existence of formation of this collation, and a portable apparatus controlling device which manages said portable apparatus corresponding by performing communication with this security control device, If said security control device performs ID registration control which records an ID code set as said portable apparatus on said recording device and there is at the time of this ID registration control, a registered signal containing an ID code used as a registering object is transmitted to said portable apparatus controlling device, A security control system, wherein this portable apparatus controlling device manages corresponding portable apparatus based on said registered signal.

[Claim 2]

If there is said security control device at the time of said ID registration control, said registered signal containing an ID code which completed registration is transmitted to said portable apparatus controlling device, It is judged whether when said portable apparatus controlling device receives said registered signal, registration of an ID code contained in this registered signal is appropriate to it, The security control system according to claim 1 performing report control which notifies an unusual reporting signal which shows that unusual registration was made to a portable transmitter machine which a user possesses when it judges that this registration is not appropriate.

[Claim 3]

If there is said security control device at the time of said ID registration control, a registration permission requirement signal is transmitted to said portable apparatus controlling device,

While judging whether registration of said ID code is appropriate to it when said portable apparatus controlling device receives said registration permission requirement signal, a reply signal which shows the decision result is transmitted to said security control device, The security control system according to claim 1 on condition that said security control device was received [ said reply signal with which registration of said ID code includes an appropriate purport ], wherein it records this ID code on said recording device.

[Claim 4]

Said portable apparatus controlling device is provided with a reception means which receives a restriction requirement signal transmitted from a portable transmitter machine which a user possesses, and on condition that this restriction requirement signal was received by this reception means, a function restriction signal is transmitted to said security control device,

A security control system given in any 1 paragraph of claims 1-3 forbidding or restricting security releasing operation by said security equipments on condition that said security control device received said function restriction signal.

[Claim 5]

A means of communication for portable apparatus which performs communication with portable apparatus with which a peculiar ID code was set up, At the time of communication with a recording device on which said ID code and a corresponding ID code are recorded, and said portable apparatus. It is a security control device provided with a security control means to control security equipments based on whether performed collation with an ID code set as portable apparatus, and an ID code recorded on said recording device, and this collation was in agreement,

A portable apparatus controlling device and a security communication means which can be communicated of managing said portable apparatus based on an ID code recorded on said recording device while being allocated in the exterior of the security control device concerned,

While performing ID registration control which records an ID code of said portable apparatus on said recording device, A security control device provided with a registration control means to perform registration communications control which transmits a registered signal containing an ID code used as this recording object to said portable apparatus controlling device via said security communication means in the case of the ID registration control.

[Claim 6]

While said registration control means transmits a registration permission requirement signal to said portable apparatus controlling device from said security communication means at the time of said ID registration control, A reply signal from said portable apparatus controlling device answered and transmitted to this registration permission requirement signal is received by said security communication means, and on condition that a purport of a registration permission is included in the reply signal, it carries out, The security control

device according to claim 5 recording said ID code on said recording device.

[Claim 7]

Said security control means carries out, on condition that a function restriction signal transmitted from said portable apparatus controlling device was received by said security communication means, The security control device according to claim 5 or 6 characterizing by forbidding or restricting security releasing operation by said security equipments.

[Claim 8]

While controlling security equipments based on a collated result of an ID code set as this portable apparatus based on communication with portable apparatus which has a communication function, and an ID code beforehand registered into self, A security control device and a management means of communication which can be communicated which transmit outside a registered signal which contains this ID code at the time of registration of said ID code,

A portable apparatus controlling device having a management tool which manages this portable apparatus based on an ID code contained in this registered signal when said management means of communication receives said registered signal.

[Claim 9]

It has a means of communication for portable devices which performs communication with a portable transmitter machine possessed by user,

It is judged whether registration of an ID code contained in this registered signal when said management means of communication receives said registered signal is appropriate to said management tool, The portable apparatus controlling device according to claim 8 performing unusual information control which makes an unusual reporting signal which shows that unusual registration was made transmit to said portable device from said means of communication for portable devices when it judges that this registration is not appropriate.

[Claim 10]

While judging whether registration of said ID code is appropriate to it when said management tool receives a registration permission requirement signal transmitted from said security control device at the time of registration of an ID code of said portable apparatus by said management means of communication, The portable apparatus controlling device according to claim 8 transmitting a reply signal which shows the decision result to said security control device.

[Claim 11]

It has a reception means which receives a restriction requirement signal transmitted from a portable transmitter machine which a user possesses,

Said management tool carries out, on condition that said restriction requirement signal was received by said reception means, The portable apparatus controlling device according to claim 8 to 10 transmitting a function restriction signal for making security releasing operation by said security equipments forbid or restrict to either [ at least ] said security

control device or said portable apparatus.

[Claim 12]

Communication with portable apparatus which has a communication function performs collation with an ID code set as portable apparatus, and an ID code already recorded on an own recording device, It is the security control method in a security control system provided with a security control device which controls security equipments based on existence of enactment of this collation, and a portable apparatus controlling device which manages said portable apparatus by performing communication with this security control device, Said security control device performs ID registration control which records an ID code set as said portable apparatus on said recording device, and a registered signal containing an ID code used as a registering object is transmitted to said portable apparatus controlling device from this security control device at the time of this ID registration control, A security control method managing an ID code contained in said registered signal, and corresponding portable apparatus with said portable apparatus controlling device.

---

[Translation done.]

**\* NOTICES \***

JP0 and INPIT are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.\*\*\*\* shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

---

**DETAILED DESCRIPTION**

---

[Detailed Description of the Invention]

[Field of the Invention]

[0001]

This invention relates to the security control system, security control device and portable apparatus controlling device which are used for vehicles, a residence, etc., for example, and the security control method.

[Background of the Invention]

[0002]

Generally, it is operational in security equipments, such as vehicles and a door lock device of a residence, using the machine key for exclusive use possessed by the user. However, since there is a possibility that security equipments may be unjustly operated by copying a machine key unjustly in this case, or performing picking etc., it is regarded as questionable socially.

[0003]

Then, in order to aim at improvement in the security level of security equipments conventionally, the security control system which used electronic collation, for example is proposed (for example, refer to the patent documents 1 and patent documents 2).

[0004]

As shown in these patent documents 1 and 2, in the security control system for vehicles, radio is performed between the portable apparatus possessed by the user and the security control device allocated by vehicles. If the ID code signal which specifically contains the peculiar ID code set as portable apparatus is transmitted to a security control device from portable apparatus, a security control device will perform comparison with the ID code contained in this ID code signal, and the ID code beforehand registered into self. And when these ID codes of a security control device correspond, it judges that communication with portable apparatus was materialized, makes a door lock unlock or performs engine start-up permission. That is, a security control device performs security releasing operation of various security equipments, on condition that communication with portable apparatus was

materialized. For this reason, the security releasing operation by the third party who does not possess corresponding portable apparatus becomes impossible, and the security level of security equipments improves.

[Patent documents 1] JP,2001-289142,A

[Patent documents 2] JP,2001-311333,A

[Description of the Invention]

[Problem(s) to be Solved by the Invention]

[0005]

By the way, in such a security control system for vehicles, communication with the portable apparatus and the vehicle control device which were mentioned above is materialized by registering the ID code of portable apparatus into the vehicle control device beforehand. For this reason, in carrying out additional registration of the portable apparatus as a spare key, for example, ID registration operation of registering the ID code of this portable apparatus is needed. Generally, in order to perform this ID registration operation, it is necessary to switch a vehicle control device to ID registration mode, and to perform communication with portable apparatus and a vehicle control device in this ID registration mode by performing predetermined operation. And an operating procedure for ID registration operation to be performed by a dealer etc. and only for a specific worker switch to ID registration mode conventionally, can be known now.

[0006]

However, in the conventional security control device for vehicles, if it gets to know, and it is clear and the work sequence of ID registration operation of portable apparatus of what can acquire the theft preventive effect outstanding in the anticipated-use state is, the unjust ID registration of portable apparatus will become possible. Thus, in the conventional security control system for vehicles, although it is a special case, a thoroughgoing theft preventive effect may not be acquired.

[0007]

When a user loses the portable apparatus which completed registration of the ID code or the theft of this portable apparatus is carried out, there is a possibility that this portable apparatus may be used by the third party.

So, in the former, it is requested that the security level of security equipments is made still higher.

[0008]

This invention is made in view of such the actual condition, and the purpose is to provide the security control system, security control device and portable apparatus controlling device which can raise the security level of security equipments further, and the security control method.

[Means for Solving the Problem]

[0009]

In order to solve the above-mentioned technical problem, in the invention according to



claim 1. Communication with portable apparatus which has a communication function performs collation with an ID code set as portable apparatus, and an ID code already recorded on an own recording device, By performing communication with a security control device which controls security equipments based on existence of formation of this collation, and this security control device, Are a portable apparatus controlling device which manages said corresponding portable apparatus the security control system which it had, and said security control device, If ID registration control which records an ID code set as said portable apparatus on said recording device is performed and it is at the time of this ID registration control, Transmitting a registered signal containing an ID code used as a registering object to said portable apparatus controlling device, this portable apparatus controlling device makes it a gist to manage corresponding portable apparatus based on said registered signal.

[0010]

In the invention according to claim 2, in the security control system according to claim 1, said security control device, If it is at the time of said ID registration control, transmit to said portable apparatus controlling device, and said registered signal containing an ID code which completed registration said portable apparatus controlling device, When you judge whether registration of an ID code contained in this registered signal is appropriate when said registered signal is received and you judge that this registration is not appropriate, let it be a gist to perform report control which notifies an unusual reporting signal which shows that unusual registration was made to a portable transmitter machine which a user possesses.

[0011]

In the invention according to claim 3, in the security control system according to claim 1, said security control device, If it is at the time of said ID registration control, transmit to said portable apparatus controlling device, and a registration permission requirement signal said portable apparatus controlling device, When said registration permission requirement signal is received, while judging whether registration of said ID code is appropriate, Transmitting a reply signal which shows the decision result to said security control device, said security control device makes it a gist for registration of said ID code to record this ID code on said recording device, on condition that said reply signal including an appropriate purport was received.

[0012]

In the invention according to claim 4, in any 1 paragraph of claims 1-3, in a security control system of a statement said portable apparatus controlling device, It has a reception means which receives a restriction requirement signal transmitted from a portable transmitter machine which a user possesses, On condition that this restriction requirement signal was received by this reception means, transmit to said security control device, and a function restriction signal said security control device, Let it be a gist to forbid or restrict security releasing operation by said security equipments, on condition that said function restriction

signal was received.

[0013]

A means of communication for portable apparatus which performs communication with portable apparatus with which a peculiar ID code was set up in the invention according to claim 5, At the time of communication with a recording device on which said ID code and a corresponding ID code are recorded, and said portable apparatus. Collation with an ID code set as portable apparatus and an ID code recorded on said recording device is performed, While being a security control device provided with a security control means to control security equipments based on whether this collation was in agreement and being allocated in the exterior of the security control device concerned, While performing ID registration control which records a portable apparatus controlling device and a security communication means which can be communicated of managing said portable apparatus based on an ID code recorded on said recording device, and an ID code of said portable apparatus on said recording device, Let it be a gist to have a registration control means to perform registration communications control which transmits a registered signal containing an ID code used as this recording object to said portable apparatus controlling device via said security communication means in the case of the ID registration control.

[0014]

In the invention according to claim 6, in the security control device according to claim 5, said registration control means, While transmitting a registration permission requirement signal to said portable apparatus controlling device from said security communication means at the time of said ID registration control, A reply signal from said portable apparatus controlling device answered and transmitted to this registration permission requirement signal is received by said security communication means, and let it be a gist to record said ID code on said recording device, on condition that a purport of a registration permission is included in the reply signal.

[0015]

In the invention according to claim 7, in the security control device according to claim 5 or 6, said security control means, Let it be a gist to be characterized by forbidding or restricting security releasing operation by said security equipments, on condition that a function restriction signal transmitted from said portable apparatus controlling device was received by said security communication means.

[0016]

While controlling security equipments by the invention according to claim 8 based on a collated result of an ID code set as this portable apparatus based on communication with portable apparatus which has a communication function, and an ID code beforehand registered into self, A security control device and a management means of communication which can be communicated which transmit outside a registered signal which contains this ID code at the time of registration of said ID code, When said management means of communication receives said registered signal, let it be a gist to have a management tool

which manages this portable apparatus based on an ID code contained in this registered signal.

[0017]

Have a means of communication for portable devices which performs communication with a portable transmitter machine possessed by user in the portable apparatus controlling device according to claim 8 in the invention according to claim 9, and said management tool, It is judged whether registration of an ID code contained in this registered signal when said management means of communication receives said registered signal is appropriate, When you judge that this registration is not appropriate, let it be a gist to perform unusual information control which makes an unusual reporting signal which shows that unusual registration was made transmit to said portable device from said means of communication for portable devices.

[0018]

In the invention according to claim 10, in the portable apparatus controlling device according to claim 8, said management tool, When said management means of communication receives a registration permission requirement signal transmitted from said security control device at the time of registration of an ID code of said portable apparatus, while judging whether registration of said ID code is appropriate, Let it be a gist to transmit a reply signal which shows the decision result to said security control device.

[0019]

In the portable apparatus controlling device according to claim 8 to 10 by the invention according to claim 11, Have a reception means which receives a restriction requirement signal transmitted from a portable transmitter machine which a user possesses, and said management tool, Let it be a gist to transmit a function restriction signal for making security releasing operation by said security equipments forbid or restrict, on condition that said restriction requirement signal was received by said reception means to either [ at least ] said security control device or said portable apparatus.

[0020]

In the invention according to claim 12, by communication with portable apparatus which has a communication function. A security control device which performs collation with an ID code set as portable apparatus, and an ID code already recorded on an own recording device, and controls security equipments based on existence of formation of this collation, It is the security control method in a security control system provided with a portable apparatus controlling device which manages said portable apparatus by performing communication with this security control device, Said security control device performs ID registration control which records an ID code set as said portable apparatus on said recording device, Let it be a gist to transmit a registered signal containing an ID code used as a registering object from this security control device to said portable apparatus controlling device, and to manage an ID code contained in said registered signal, and corresponding portable apparatus with said portable apparatus controlling device at the

time of this ID registration control.

[0021]

Hereafter, "OPERATION" of this invention is explained.

According to the invention according to claim 1 or 12, a security control device controls security equipments based on whether communication with portable apparatus was materialized. And in order to form communication with portable apparatus and a security control device, ID registration which records an ID code of portable apparatus on a recording device of a security control device is needed. At the time of this ID registration, a registered signal containing an ID code used as a registering object is transmitted to a portable apparatus controlling device from a security control device. And a portable apparatus controlling device manages corresponding portable apparatus based on this registered signal. For this reason, when an ID code of portable apparatus is unjustly registered into a security control device, recognition of this unjust registration is attained with a portable apparatus controlling device. therefore, for example, when unjust registration of an ID code is performed, make that notify from a portable apparatus controlling device, or. Based on communication with this portable apparatus by which unjust registration was carried out, it becomes possible to make a portable apparatus controlling device perform restriction control prevented from controlling security equipments of a security control device. So, it becomes possible to raise a security level of security equipments further.

[0022]

If an ID code of portable apparatus is unjustly registered into a security control device according to the invention according to claim 2, an unusual reporting signal which shows that unusual registration was made will be notified to a portable transmitter machine which a user possesses from a portable apparatus controlling device. For this reason, the user can recognize certainly and promptly that an ID code of portable apparatus was registered unjustly through a portable transmitter machine. Therefore, a prompt action over this unjust registration is attained, and it becomes possible to raise a security level of security equipments further.

[0023]

If it is at the time of ID registration control according to the invention according to claim 3, A judgment whether registration of an ID code used as a registering object is appropriate is made by a portable apparatus controlling device, and unless registration of this ID code is judged to be appropriate, the security control device cannot record this ID code on a recording device. For this reason, unjust registration of an ID code is deterred and a security level of security equipments improves.

[0024]

If a restriction requirement signal which is transmitted from a portable transmitter machine which a user possesses according to the invention according to claim 4 is received by portable apparatus controlling device, a function restriction signal will be transmitted from a

portable apparatus controlling device to a security control device. A security control device forbids or restricts security releasing operation by security equipments, on condition that a function restriction signal was received. For this reason, when a user loses portable apparatus or a theft is carried out, security releasing operation can be forbidden or restricted by making a restriction requirement signal transmit from a portable transmitter machine. Therefore, also in the time of loss and a theft of portable apparatus, security releasing operation by this portable apparatus can be forbidden or restricted immediately, and a high security level of security equipments can be secured.

[0025]

According to the invention according to claim 5, a security control device controls security equipments based on whether communication with portable apparatus was materialized. And in order to form communication with portable apparatus and a security control device, ID registration which records an ID code of portable apparatus on a recording device of a security control device is needed. At the time of this ID registration, a registered signal containing an ID code used as a registering object is transmitted to a portable apparatus controlling device from a security control device. Thereby, a portable apparatus controlling device becomes possible [ managing corresponding portable apparatus based on this registered signal ]. For this reason, when an ID code of portable apparatus is unjustly registered into a security control device, recognition of this unjust registration is attained with a portable apparatus controlling device. therefore, for example, when unjust registration of an ID code is performed, make that notify from a portable apparatus controlling device, or. Based on communication with this portable apparatus by which unjust registration was carried out, it becomes possible to make a portable apparatus controlling device perform restriction control prevented from controlling security equipments of a security control device. So, it becomes possible to raise a security level of security equipments further.

[0026]

According to the invention according to claim 6, if it is at the time of ID registration control, a registration permission requirement signal is transmitted to a portable apparatus controlling device from a security communication means. And a registration control means does not record an ID code of portable apparatus used as a registering object on a recording device, unless a security communication means receives a reply signal including a purport of a registration permission transmitted from a portable apparatus controlling device. That is, in order for a registration control means to record an ID code of portable apparatus on a recording device, permission by a portable apparatus controlling device is needed, and an ID code cannot be registered only by communication with portable apparatus and a security control device. Therefore, unjust registration of an ID code is deterred and a security level of security equipments improves further.

[0027]

If a function restriction signal is transmitted from a portable apparatus controlling device to

a security control device according to the invention according to claim 7, a security control device will forbid or restrict security releasing operation by security equipments. For this reason, when a user loses portable apparatus or a theft is carried out, security releasing operation can be forbidden or restricted by making a function restriction signal transmit to a security control device from a portable apparatus controlling device. Therefore, also in the time of loss and a theft of portable apparatus, security releasing operation by this portable apparatus can be forbidden or restricted immediately, and a high security level of security equipments can be secured.

[0028]

According to the invention according to claim 8, a registered signal transmitted from a security control device is received by management means of communication. And management of this portable apparatus based on an ID code peculiar to portable apparatus contained in the registered signal is performed by management tool. So, recognition of an ID code registered into a security control device of a management tool is attained, and when an ID code of portable apparatus is unjustly registered into a security control device, recognition of that of it is attained. therefore, for example, when unjust registration of an ID code is performed, make that notify from a portable apparatus controlling device, or. Based on communication with this portable apparatus by which unjust registration was carried out, it becomes possible to make a portable apparatus controlling device perform restriction control prevented from controlling security equipments of a security control device. So, it becomes possible to raise a security level of security equipments further.

[0029]

When it is judged according to the invention according to claim 9 that registration of an ID code of portable apparatus to a security control device is not appropriate to a management tool, it is judged that an ID code was unjustly registered into a security control device. And an unusual reporting signal which shows that unusual registration was made in this case is transmitted to a portable transmitter machine which a user possesses from a portable apparatus controlling device. For this reason, the user can recognize certainly and promptly that an ID code of portable apparatus was registered unjustly through a portable transmitter machine. Therefore, a prompt action over this unjust registration is attained, and it becomes possible to raise a security level of security equipments further.

[0030]

According to the invention according to claim 10, if it is at the time of registration to a security control device of an ID code of portable apparatus, a judgment whether registration of an ID code used as a registering object is appropriate is made by a management tool, and a reply signal which shows the decision result is transmitted to a security control device. For this reason, if a security control device is constituted so that an ID code cannot be registered unless a reply signal which shows a decision result of a purport that registration of an ID code is appropriate, for example is received, Unless registration of an ID code is judged to be appropriate by a management tool, this ID code cannot be

registered. Therefore, unjust registration of an ID code is deterred and a security level of security equipments improves further.

[0031]

If according to the invention according to claim 11 a security control device is constituted so that security releasing operation by security equipments may be forbidden or restricted, on condition that a function restriction signal was received, for example, If a user makes a restriction requirement signal transmit from a portable transmitter machine, it will become possible to make this security releasing operation forbid or restrict easily of him. If portable apparatus is constituted so that communication with a security control device may be forbidden, on condition that a function restriction signal was received, for example and a user will make a limiting signal transmit from a portable transmitter machine, it will become possible to make this security releasing operation forbid or restrict easily.

[Effect of the Invention]

[0032]

As explained in full detail above, according to this invention, the security level of security equipments can be raised further.

[Best Mode of Carrying Out the Invention]

[0033]

(A 1st embodiment)

Hereafter, a 1st embodiment that materialized this invention to the security control system for vehicles is described in detail based on drawing 1 and drawing 2.

[0034]

As shown in drawing 1, the security control system 1 for vehicles is provided with the following.

Portable apparatus 3 possessed by the user (owner) of the vehicles 2.

The security control device 10 formed in the vehicles 2.

The portable apparatus controlling device 30 formed in the prescribed spot of the vehicles exterior.

[0035]

The portable apparatus 3 has a communication function and serves as ability ready for receiving in the request signal transmitted from the security control device 10. And the portable apparatus 3 will transmit the ID code signal containing the ID code beforehand set as self, if this request signal is received. The portable apparatus 3 will transmit the lock/unlock command signal containing an ID code, and a locking code or a unlocking code, if the final controlling element provided in self is operated.

[0036]

The security control device 10 is provided with the following.

The sending circuit 11 and the receiving circuit 12 as a means of communication for portable apparatus.

The vehicle control part 13 as a security control means and a registration control means.

The security communication part 14 as a security communication means.

And the sending circuit 11, the receiving circuit 12, and the security communication part 14 are electrically connected to the vehicle control part 13.

[0037]

The sending circuit 11 changes into the electric wave of predetermined frequency (here 134 kHz) the request signal outputted from the vehicle control part 13, and transmits this electric wave to the surrounding predetermined region of the vehicles 2, and the interior of a room of the vehicles 2 selectively via the transmission antenna 11a.

[0038]

The receiving circuit 12 receives the ID code signal and lock/unlock command signal which are transmitted from the portable apparatus 3 via the receiving antenna 12a, restores to the input signal to a pulse signal, and outputs it to the vehicle control part 13.

[0039]

The security communication part 14 is constituted so that the portable apparatus controlling device 30 and communication are possible. And if a registered signal is inputted from the vehicle control part 13, the security communication part 14 will modulate the registered signal on the electric wave of predetermined frequency, and will transmit this electric wave to the portable apparatus controlling device 30. It will restore to this sending signal to a pulse signal, and the security communication part 14 will output the signal to which it this restored to the vehicle control part 13, if the sending signal transmitted from the portable apparatus controlling device 30 is received.

[0040]

The vehicle control part 13 is a CPU unit which consists of CPU, ROM, and RAM which are not illustrated, and is specifically provided with the nonvolatile memory 13a as a recording device. In this memory 13a, one or more records of the ID code set as the portable apparatus 3 are possible.

[0041]

The mode switch 21, and the door lock drive device 22 and Engine control section 23 as security equipments are electrically connected to the vehicle control part 13.

The mode switch 21 is an operational switch and is provided in the interior of a room of the vehicles 2 by the user in this embodiment. And operation of this mode switch 21 will output a manipulate signal to these mode switch 21 empty-vehicle both control sections 13.

[0042]

If it is connected to the actuator which is not illustrated and a driving signal is inputted from the vehicle control part 13, the door lock drive device 22 will drive this actuator, and will carry out lock/unlock of the door lock automatically. The door lock drive device 22 outputs the lock/unlock condition signal which shows the lock/unlock state of a door lock to the vehicle control part 13. For this reason, based on this lock/unlock condition signal, recognition of the lock/unlock state of a door lock of the vehicle control part 13 is attained.



[0043]

It performs fuel injection control and ignition control, and starts an engine automatically while driving the starter, if it is connected to the starter which is not illustrated and Engine control section 23 is inputted [ a start signal ] from the vehicle control part 13. Engine control section 23 outputs the driving state signal which shows an engine driving state to the vehicle control part 13. For this reason, based on this driving state signal, recognition of an engine driving state of the vehicle control part 13 is attained.

[0044]

The vehicle control part 13 is provided with the following.

Security control mode which controls the door lock drive device 22 and Engine control section 23.

ID registration mode in which ID registration control which records the ID code set as the portable apparatus 3 on the memory 13a (registration) is performed.

And the vehicle control part 13 serves as ID registration mode, when a manipulate signal is inputted from the mode switch 21, and it serves as security control mode except it.

[0045]

In security control mode, the vehicle control part 13 outputs a request signal intermittently to the sending circuit 11. For this reason, a request signal is selectively transmitted to the surrounding predetermined region of the vehicles 2, and the interior of a room of the vehicles 2 via the sending circuit 11 and the transmission antenna 11a. The vehicle control part 13 will perform comparison (ID code collation) with the ID code contained in those signals, and the ID code currently recorded on the memory 13a, if said ID code signal or a lock/unlock command signal is inputted from the receiving circuit 12. And the vehicle control part 13 performs drive controlling of the door lock drive device 22 or Engine control section 23, on condition that these ID codes were in agreement, i.e., collation of the ID code was materialized.

[0046]

When an ID code signal is inputted, the vehicle control part 13 outputs a driving signal to the door lock drive device 22, and makes a door lock unlock in detail, if this ID code signal answers the request signal transmitted to the surrounding predetermined region of the vehicles 2. And if this ID code signal is no longer inputted, the vehicle control part 13 outputs a driving signal to the door lock drive device 22, and makes a door lock lock.

[0047]

On the other hand, the vehicle control part 13 will be in an engine start waiting state, if the inputted ID code signal answers the request signal transmitted to the interior of a room of the vehicles 2. And if a manipulate signal is inputted from the start switch which is not illustrated in this engine start waiting state, the vehicle control part 13 will output a start signal to Engine control section 23, and will start an engine. That is, when it is not an engine start waiting state, the vehicle control part 13 will not output a start signal to Engine control section 23, even if a manipulate signal is inputted from a start switch. A start switch

is a switch formed near the driver's seat in the interior of a room of the vehicles 2, and is electrically connected with the vehicle control part 13.

[0048]

The vehicle control part 13 will make a door lock lock, if the locking code is contained in this lock/unlock command signal, and if the unlocking code is contained, it will make a door lock unlock, when a lock/unlock command signal is inputted.

[0049]

Thus, in security control mode, the security control device 10 performs communication with the portable apparatus 3, and controls security equipments, such as the door lock drive device 22 and Engine control section 23, based on the formation existence of communication with this portable apparatus 3.

[0050]

On the other hand, if it switches from security control mode to ID registration mode, the vehicle control part 13 will output a request signal intermittently to the sending circuit 11, and will perform communication with the portable apparatus 3 like security control mode. And the vehicle control part 13 will record the ID code contained in this ID code signal on the memory 13a, if an ID code signal is inputted from the receiving circuit 12. If this record is completed, the vehicle control part 13 will output the registered signal which includes this ID code and vehicle information to the security communication part 14, and will perform registration communications control which transmits a registered signal to the portable apparatus controlling device 30 via this security communication part 14. Vehicle information is information for specifying the vehicles 2, and at least one of the car body number of the vehicles 2, a fleet number, and dealer information, including a store number, a password, etc. which were set up peculiar to a dealer, is contained in vehicle information in this embodiment.

[0051]

The portable apparatus controlling device 30 is allocated in the control center for exclusive use etc., and is provided with the management communications department 31 as a management means of communication, the supervisory control part 32 as a management tool, and the communications department 33 for portable devices as a means of communication for portable devices. And the management communications department 31 and the communications department 33 for portable devices are electrically connected to the supervisory control part 32.

[0052]

The security communication part 14 of the security control device 10 and communication of the management communications department 31 are attained, and if the registered signal transmitted from this security communication part 14 is received, it will restore to the registered signal and will output to the supervisory control part 32.

[0053]

The portable transmitter machine (here cellular phone 4) possessed by the user and

communication are possible for the communications department 33 for portable devices. And the communications department 33 for portable devices will transmit the unusual reporting signal to the cellular phone 4 using a public network etc., if an unusual reporting signal is inputted from the supervisory control part 32.

[0054]

The supervisory control part 32 is a CPU unit which consists of CPU, ROM, and RAM which are not illustrated, and is specifically provided with the nonvolatile memory 32a. The vehicle information of the vehicles 2 set up as an administration object, the registration yes-or-no information set up corresponding to this vehicle information, and the ID code recorded on the memory 13a of the security control device 10 carried in these vehicles 2 are recorded on this memory 32a. In detail, the information for specifying the vehicles 2, including the car body number of the vehicles 2, a fleet number, dealer information, the equipment information (a telephone number, a mail address, etc.) of said cellular phones (a store number, a password, etc. which were set up peculiar to a dealer) 4, etc., is recorded on the memory 32a as vehicle information.

[0055]

Registration yes-or-no information is information which shows whether registration of an ID code is approved, or it is considered as disapproval, and is transmitted from the cellular phone 4. This registration yes-or-no information can be set up by a user. Registration yes-or-no information consists of a password cord of a predetermined digit number, and, specifically, is equivalent to what carried out binary conversion of the password inputted from the ten key of the cellular phone 4. Two kinds such as the registration authorization code which approves registration of an ID code, and the registration disapproval code which makes registration of an ID code disapproval exist, and this registration yes-or-no information corresponds with the password which can be set up by a user, respectively. For this reason, the user can set up freely the password as a registration authorization code, and the password as a registration disapproval code. When predetermined yes-or-no transmitting information operations (for example, a telephone number input, predetermined command input, etc. to the portable apparatus controlling device 30) are performed in this embodiment as for the cellular phone 4, registration yes-or-no information is transmitted to the portable apparatus controlling device 30.

[0056]

Corresponding to this vehicle information, the record section of an ID code and the record section of registration yes-or-no information are set to the memory 32a. For example, when the vehicle information A and B of the two vehicles 2 is recorded on the memory 32a, the record section of the ID code corresponding to the vehicle information A and the record section of registration yes-or-no information, and the record section of the ID code corresponding to the vehicle information B and the record section of registration yes-or-no information are set up individually. It is a record section of this ID code recordable about two or more ID codes, and the number of the ID codes in which the record is possible is the

prescribed number set up by the prescribed number set up beforehand or the user. The registration number which consists of turn etc. which were recorded, for example is matched with the ID code recorded on this record section.

[0057]

The supervisory control part 32 will record the registration yes-or-no information on the memory 32a, if the registration yes-or-no information transmitted from the cellular phone 4 is inputted via the communications department 33 for portable devices. The supervisory control part 32 carries out renewal record (overwriting) of the newest registration yes-or-no information to the memory 32a, whenever registration yes-or-no information is inputted.

[0058]

If a registered signal is inputted from the management communications department 31, the supervisory control part 32, The registration yes-or-no information that it corresponds based on the vehicle information included in this registered signal is a registration authorization code, and when free space exists in the record section of a corresponding ID code, the ID code contained in the registered signal is recorded on this free space. That is, it is judged in such a case that registration of an ID code is appropriate to the supervisory control part 32. And the supervisory control part 32 transmits the registration completion signal which shows that this record was completed to the security control device 10 via the management communications department 31. On the other hand, the supervisory control part 32 judges that unusual registration of the ID code was performed, when there is no free space in the record section of vehicle information and a corresponding ID code, or when the registration yes-or-no information that it corresponds is a registration disapproval code. That is, it is judged in such a case that registration of an ID code is not appropriate to the supervisory control part 32. And the supervisory control part 32 outputs the unusual reporting signal which shows that this unusual registration was performed to the communications department 33 for portable devices. Therefore, an unusual reporting signal is transmitted to the cellular phone 4 from the communications department 33 for portable devices.

[0059]

Next, in the security control system 1 for vehicles constituted in this way, the communication mode performed when registering the ID code of the portable apparatus 3 into the security control device 10 is explained using the sequence chart shown in drawing 2.

[0060]

First, if the mode switch 21 of the security control device 10 is operated by the user (Step S1), the security control device 10 will switch from security control mode to ID registration mode (Step S2). If it switches to ID registration mode, the security control device 10 will transmit said request signal to the interior of a room of the vehicles 2 (Step S3).

[0061]

And the portable apparatus 3 will transmit said ID code signal, if this request signal is received (step S4).

The security control device 10 will record the ID code contained in this ID code signal on the memory 13a, if the ID code signal from the portable apparatus 3 is received (Step S5). That is, the security control device 10 registers the ID code of the acquired portable apparatus 3 into self. Subsequently, the security control device 10 transmits said registered signal to the portable apparatus controlling device 30 (Step S6).

[0062]

The portable apparatus controlling device 30 will judge whether registration of the ID code to the corresponding security control device 10 is certificate voice based on the vehicle information included in this registered signal, if the registered signal from the security control device 10 is received (Step S7). That is, the portable apparatus controlling device 30 judges here whether the registration yes-or-no information corresponding to vehicle information is a registration authorization code. It is judged whether the portable apparatus controlling device 30 can record the ID code which deduces the record section of the ID code in the memory 32a, and is contained in a registered signal on this record section (the step S7). That is, the portable apparatus controlling device 30 judges here whether the field which can register an ID code into this record section exists. As a result, when the registration yes-or-no information that it corresponds is a registration authorization code and free space exists in the storage area of vehicle information and a corresponding ID code in the memory 32a, It judges that registration of an ID code is appropriate to the portable apparatus controlling device 30, and the acquired ID code is recorded on this free space (Step S8). The portable apparatus controlling device 30 transmits said registration completion signal to the security control device 10 (step S9). For this reason, the portable apparatus controlling device 30 becomes manageable [ the portable apparatus 3 corresponding to the vehicles 2 ] based on the recorded ID code.

[0063]

If the registration completion signal from the portable apparatus controlling device 30 is received, the security control device 10 will perform the display which shows the purport of registration completion to the indicator which was formed in the interior of a room of the vehicles 2, and which is not illustrated, or will perform sound information which shows the purport of this registration completion from the loudspeaker etc. which are not illustrated (Step S10). For this reason, recognition of a user is certainly attained [ that registration of the portable apparatus 3 was completed, and ].

[0064]

The case where the registration yes-or-no information on Step S7 and corresponding to vehicle information in the portable apparatus controlling device 30 is a registration disapproval code on the other hand, When the field which can register an ID code into the record section of a corresponding ID code does not exist, it judges that registration of an ID code is not appropriate, and said unusual reporting signal is transmitted to the cellular phone 4 (Step S11). For this reason, it is shown that the cellular phone 4 had unusual registration of an ID code. Therefore, for example, when registration of an ID code is

unjustly performed by the third party, even if the user has estranged from vehicles, he can recognize the purport of this unjust registration promptly and certainly.

[0065]

Therefore, according to this embodiment, the following effects can be acquired.

(1) The security control device 10 controls security equipments, such as the door lock drive device 22 and Engine control section 23, based on whether communication with the portable apparatus 3 was materialized. And in order to form communication with the portable apparatus 3 and the security control device 10, the ID registration which records the ID code of the portable apparatus 3 on the memory 13a of the vehicle control part 13 of the security control device 10 is needed. At the time of this ID registration, the registered signal containing the ID code used as a registering object is transmitted to the portable apparatus controlling device 30 from the security control device 10. And the portable apparatus controlling device 30 will manage the portable apparatus 3 which records the ID code contained in this registered signal on the memory 32a of the supervisory control part 32, and corresponds based on the this recorded ID code, if this registered signal is received. For this reason, when the ID code of the portable apparatus 3 is unjustly registered into the security control device 10, this unjust registration can be recognized with the portable apparatus controlling device 30. Therefore, unjust registration of the ID code by a third party can be deterred, and the security level of security equipments can be raised further.

[0066]

(2) When the registration yes-or-no information which becomes the memory 32a of the supervisory control part 32 in the portable apparatus controlling device 30 from a registration disapproval code is recorded, the portable apparatus controlling device 30 will be in the registration disapproval state which makes disapproval registration of the ID code to the security control device 10. However, if a registered signal is inputted from the security control device 10 in spite of this registration disapproval state, the portable apparatus controlling device 30 will judge that unjust registration of the ID code was performed, and will notify that to the cellular phone 4. That is, when unjust registration of an ID code is performed, that is notified to the cellular phone 4. For this reason, even if the user has estranged from the vehicles 2, he can recognize promptly and certainly that unjust registration of the ID code was performed through the cellular phone 4, and the prompt action of him over this unjust registration will be attained. Therefore, the security level of security equipments can be raised further.

[0067]

(3) If a password is inputted into the cellular phone 4, registration yes-or-no information will be transmitted from this cellular phone 4 to the portable apparatus controlling device 30. And the portable apparatus controlling device 30 switches to either the registration certificate voice of an ID code or the registration disapproval states of an ID code based on this registration yes-or-no information. That is, the registration certificate voice of the ID

code in the portable apparatus controlling device 30 and a registration disapproval state can be set up by a user. For this reason, the user can make the portable apparatus controlling device 30 registration certificate voice, for example, only when registration of an ID code is required. Therefore, the security level of security equipments can be raised further.

[0068]

(4) At the time of the registration completion of the ID code to the security control device 10 and the portable apparatus controlling device 30, that is displayed on the indicator formed in the interior of a room of the vehicles 2. For this reason, the user can recognize certainly that registration of the ID code was completed by recognizing this indicator visually.

[0069]

(A 2nd embodiment)

Next, a 2nd embodiment that materialized this invention is described based on drawing 1 and drawing 3. In each following embodiment, it only supposes that it is to mainly describe the point which is different from a 1st embodiment, and to attach the same member number about a common point, and the explanation is omitted.

[0070]

A different point from said 1st embodiment in this embodiment, The control mode performed by the vehicle control part 13 of the security control device 10, and the supervisory control part 32 of the portable apparatus controlling device 30, It is about the communication mode of the security control system 1 for vehicles performed at the time of the control (ID registration control) which registers the ID code of the portable apparatus 3 into the security control device 10. About the hardware constitutions of the portable apparatus 3, the security control device 10, and the portable apparatus controlling device 30, it is the same as a 1st embodiment.

[0071]

Then, the control first performed by the vehicle control part 13 and the supervisory control part 32 is explained.

The vehicle control part 13 performs the same control as said 1st embodiment in security control mode. On the other hand, if the mode switch 21 is operated and it switches from security control mode to ID registration mode, the vehicle control part 13 will output a registration permission requirement signal including vehicle information to the security communication part 14. For this reason, this registration permission requirement signal is transmitted to the portable apparatus controlling device 30 from the security communication part 14 (refer to drawing 1).

[0072]

The vehicle control part 13 will judge whether the authorization code is contained in this reply signal, if a reply signal is inputted from the security communication part 14 after outputting a registration permission requirement signal. And if the vehicle control part 13 judges that the authorization code is contained in this reply signal, it will output a request

signal intermittently to the sending circuit 11, and will perform communication with the portable apparatus 3 like said 1st embodiment. And the vehicle control part 13 will record the ID code contained in this ID code signal on the memory 13a, if the ID code signal transmitted from the portable apparatus 3 is inputted from the receiving circuit 12. If this record is completed, the vehicle control part 13 will output the registered signal which includes this ID code and vehicle information to the security communication part 14, and will transmit this registered signal to the portable apparatus controlling device 30 via this security communication part 14.

[0073]

On the other hand, it performs the display which shows that registration of an ID code is a prohibited state to the indicator which was formed in the interior of a room of the vehicles 2, and which is not illustrated while forbidding communication with the portable apparatus 3 in ID registration mode, when the vehicle control part 13 cannot be received [ the reply signal containing this authorization code ]. For this reason, if it is in the state where registration of the ID code is forbidden by the portable apparatus controlling device 30, a new ID code is not recorded on the memory 13a of the vehicle control part 13. Recognition of a user is certainly attained in the purport that this record is forbidden, by recognizing an indicator visually.

[0074]

On the other hand, if the registration permission requirement signal from the security control device 10 is inputted, the supervisory control part 32, The vehicle information included in this registration permission requirement signal among the registration yes-or-no information currently recorded on the memory 32a and the registration yes-or-no information that it corresponds are registration authorization codes, and it is judged whether free space exists in the record section of a corresponding ID code (attestation). And if this attestation is materialized, the supervisory control part 32 will transmit the reply signal containing an authorization code to the security control device 10 via the management communications department 31 (refer to drawing 1). On the other hand, when this attestation is not materialized (i.e., when there is no free space in the record section of vehicle information and a corresponding ID code), and when the registration yes-or-no information that it corresponds is a registration disapproval code, the supervisory control part 32 does not transmit a reply signal. Furthermore, in this case, the supervisory control part 32 judges that unusual registration of an ID code tends to be performed, and outputs the unusual reporting signal which shows that to the communications department 33 for portable devices. Therefore, an unusual reporting signal is transmitted to the cellular phone 4 from the communications department 33 for portable devices.

[0075]

The supervisory control part 32 will record the ID code contained in the registered signal on this free space, if a registered signal is inputted from the security control device 10 via the management communications department 31. And the supervisory control part 32 transmits



the registration completion signal which shows that this record was completed to the security control device 10 via the management communications department 31.

[0076]

Next, the communication mode at the time of ID registration control of the security control system 1 for vehicles of this embodiment is explained using the sequence chart shown in drawing 3.

First, if the mode switch 21 of the security control device 10 is operated by the user (Step S21), the security control device 10 will switch from security control mode to ID registration mode (Step S22). If it switches to ID registration mode, the security control device 10 will transmit a registration permission requirement signal to the portable apparatus controlling device 30 (Step S23).

[0077]

The portable apparatus controlling device 30 will judge whether registration of the ID code to the corresponding security control device 10 is certificate voice based on the vehicle information included in this registration permission requirement signal, if this registration permission requirement signal is received (Step S24). (attestation) That is, the portable apparatus controlling device 30 judges here whether the registration yes-or-no information corresponding to vehicle information is a registration authorization code. It is judged whether the portable apparatus controlling device 30 can deduce the record section of the ID code in the memory 32a, and can newly record an ID code on this record section (the step S24). That is, the portable apparatus controlling device 30 judges here whether the field which can register a new ID code into this record section exists. As a result, when the registration yes-or-no information that it corresponds is a registration authorization code and free space exists in the storage area of vehicle information and a corresponding ID code in the memory 32a, It judges that registration of an ID code is appropriate to the portable apparatus controlling device 30 (attestation O.K.), and the reply signal containing an authorization code is transmitted to the security control device 10 (Step S25).

[0078]

On the other hand, the case where the registration yes-or-no information corresponding to vehicle information in the portable apparatus controlling device 30 is a registration disapproval code, When the field which can register an ID code into the record section of a corresponding ID code does not exist, it judges that registration of an ID code is not appropriate (attestation NG), and the reply signal containing an authorization code is not transmitted to the security control device 10. The portable apparatus controlling device 30 transmits an unusual reporting signal to the cellular phone 4 in this case (Step S26). For this reason, it is shown in the cellular phone 4 that unusual registration of an ID code is going to be performed. therefore, for example, when the security control device 10 is unjustly switched to ID registration mode by the third party and it switches to ID registration mode against a user's will. Even if the user has estranged from vehicles, he can recognize promptly and certainly the purport of the transition to this ID registration mode. That is, in

this embodiment, before registering the ID code of the portable apparatus 3 into the security control device 10, unusual information is made to a user. For this reason, it becomes possible to prevent unjust registration of an ID code.

[0079]

By the way, if this reply signal is received by the security control device 10 when the reply signal which contains an authorization code from the portable apparatus controlling device 30 is transmitted, the security control device 10 will transmit said request signal to the interior of a room of the vehicles 2 (Step S27).

[0080]

And the portable apparatus 3 will transmit said ID code signal, if this request signal is received (Step S28).

The security control device 10 will record the ID code contained in this ID code signal on the memory 13a, if the ID code signal from the portable apparatus 3 is received (Step S29). That is, the security control device 10 registers the ID code of the acquired portable apparatus 3 into self. Subsequently, the security control device 10 transmits said registered signal to the portable apparatus controlling device 30 (Step S30).

[0081]

That is, in Steps S27-S30, communication equivalent to Steps S3-S6 (refer to drawing 2) in said 1st embodiment is performed.

The portable apparatus controlling device 30 will record the ID code contained in this registered signal on the free space of the record section of vehicle information and a corresponding ID code, if the registered signal from the security control device 10 is received (Step S31). The portable apparatus controlling device 30 transmits said registration completion signal to the security control device 10 (Step S32). For this reason, the portable apparatus controlling device 30 becomes manageable [ the portable apparatus 3 corresponding to the vehicles 2 ] based on the recorded ID code.

[0082]

If the registration completion signal from the portable apparatus controlling device 30 is received, the security control device 10 will perform the display which shows the purport of registration completion to the indicator which was formed in the interior of a room of the vehicles 2, and which is not illustrated, or will perform sound information which shows the purport of this registration completion from the loudspeaker etc. which are not illustrated (Step S33). For this reason, recognition of a user is certainly attained [ that registration of the portable apparatus 3 was completed, and ].

[0083]

Thus, when the security control device 10 switches to ID registration mode in this embodiment, communication with the portable apparatus controlling device 30 is performed first. As a result, when registration of an ID code is permitted by the portable apparatus controlling device 30, the security control device 10 performs communication with the portable apparatus 3, and records the ID code of the portable apparatus 3 on the memory

13a (registration). And the security control device 10 manages the ID code which performed communication with the portable apparatus controlling device 30 again, and was registered with the portable apparatus controlling device 30. For this reason, when registering the ID code of the portable apparatus 3 into the security control device 10, permission by the portable apparatus controlling device 30 is needed, and unjust registration of this portable apparatus 3 is prevented more certainly.

[0084]

Therefore, according to this embodiment, in addition to the effect of (1) in said 1st embodiment, (3), and (4), the following effects can be acquired.

(5) If it is at the time of ID registration control, a judgment whether registration of the ID code used as a registering object is appropriate is made by the portable apparatus controlling device 30, and unless registration of this ID code is judged to be appropriate, the security control device 10 cannot record this ID code on the memory 13a. That is, the security control device 10 cannot newly record the ID code of the portable apparatus 3 on the memory 13a, as long as there is no permission by the portable apparatus controlling device 30. For this reason, unjust registration of an ID code can be prevented further and the security level of security equipments can be raised further.

[0085]

(6) If the security control device 10 switches from security control mode to ID registration mode, it will ask for permission of registration of an ID code from the portable apparatus controlling device 30 first. And the security control device 10 performs communication with the portable apparatus 3, on condition that permission of this registration was made from the portable apparatus controlling device 30, and it registers the ID code of the portable apparatus 3. On the other hand, the security control device 10 performs the communication with the portable apparatus 3 itself, when permission of this registration is not made from the portable apparatus controlling device 30. That is, when registration of an ID code is impossible, communication with the portable apparatus 3 and the security control device 10 is not performed. For this reason, the useless communication with the portable apparatus 3 and the security control device 10 can be prevented, and the power consumption of the portable apparatus 3 and the security control device 10 can be reduced.

[0086]

This 2nd embodiment may be changed as follows.

- In the communications control (ID registration control) in the ID registration mode in the security control system 1 for vehicles of said 2nd embodiment. If the security control device 10 switches from security control mode to ID registration mode, it will ask for permission of registration of an ID code from the portable apparatus controlling device 30 first. And the security control device 10 performs communication with the portable apparatus 3, on condition that permission of this registration was made from the portable apparatus controlling device 30, and it registers the ID code of the portable apparatus 3. However, this ID registration control may be changed into a communication mode as shown not only in

such a communication mode but in drawing 4. Hereafter, the change mode is explained using drawing 4. In this change mode, said vehicle information and the ID code of the portable apparatus 3 used as a registering object are contained in the registration permission requirement signal outputted from the vehicle control part 13 of the security control device 10.

[0087]

First, if the mode switch 21 of the security control device 10 is operated by the user (Step S41), the security control device 10 will switch from security control mode to ID registration mode (Step S42). If it switches to ID registration mode, the security control device 10 will transmit said request signal to the interior of a room of the vehicles 2 (Step S43).

[0088]

And the portable apparatus 3 will transmit said ID code signal, if this request signal is received (Step S44).

The security control device 10 stores temporarily the ID code contained in this ID code signal at RAM, a buffer, etc., when the ID code signal from the portable apparatus 3 is received (Step S45). (provisional registration) Subsequently, the security control device 10 transmits a registration permission requirement signal including the ID code this stored temporarily and said vehicle information to the portable apparatus controlling device 30 (Step S46).

[0089]

The portable apparatus controlling device 30 will judge whether registration of the ID code to the corresponding security control device 10 is an authorized state based on the vehicle information included in this registration permission requirement signal, if this registration permission requirement signal is received (Step S47). (attestation) It is judged whether the portable apparatus controlling device 30 can deduce the record section of the ID code in the memory 32a, and can newly record an ID code on this record section (the step S47). That is, the portable apparatus controlling device 30 performs the same processing as Step S24 in said 2nd embodiment here. As a result, the registration yes-or-no information that it corresponds is a registration authorization code, and when free space exists in the storage area of vehicle information and a corresponding ID code in the memory 32a, it is judged that registration of an ID code is appropriate to the portable apparatus controlling device 30 (attestation O.K.). And the portable apparatus controlling device 30 records the ID code (acquired ID code) contained in a registration permission requirement signal on this free space of the memory 32a (Step S48). Then, the portable apparatus controlling device 30 transmits the reply signal containing an authorization code to the security control device 10 (Step S49).

[0090]

On the other hand, the case where the registration yes-or-no information corresponding to vehicle information in the portable apparatus controlling device 30 is a registration disapproval code, When the field which can register an ID code into the record section of a

corresponding ID code does not exist, it judges that registration of an ID code is not appropriate (attestation NG), and the reply signal containing an authorization code is not transmitted to the security control device 10. The portable apparatus controlling device 30 transmits an unusual reporting signal to the cellular phone 4 in this case (Step S50). For this reason, like said 2nd embodiment, before registering the ID code of the portable apparatus 3 into the security control device 10, unusual information is made to a user. Therefore, it becomes possible to prevent unjust registration of an ID code.

[0091]

By the way, if this reply signal is received by the security control device 10 when the reply signal which contains an authorization code from the portable apparatus controlling device 30 is transmitted, the security control device 10 will record said ID code stored temporarily on the memory 13a (Step S51). (high grade registry) And the security control device 10 performs the display which shows the purport of registration completion to the indicator which was formed in the interior of a room of the vehicles 2, and which is not illustrated, or performs sound information which shows the purport of this registration completion from the loudspeaker etc. which are not illustrated (Step S52). For this reason, recognition of a user is certainly attained [ that registration of the portable apparatus 3 was completed, and ].

[0092]

Thus, when the security control device 10 switches to ID registration mode in this change mode, communication with the portable apparatus controlling device 30 is performed first. As a result, when registration of an ID code is permitted by the portable apparatus controlling device 30, the security control device 10 performs communication with the portable apparatus 3, and records the ID code of the portable apparatus 3 on the memory 13a (high grade registry). And the security control device 10 manages the ID code which performed communication with the portable apparatus controlling device 30 again, and was registered with the portable apparatus controlling device 30. For this reason, when registering the ID code of the portable apparatus 3 into the security control device 10, permission by the portable apparatus controlling device 30 is needed, and unjust registration of this portable apparatus 3 is prevented more certainly.

[0093]

The ID code of the acquired portable apparatus 3 is contained in a registration permission requirement signal, and if it is judged as the attestation O.K. while this registration permission requirement signal is received by the portable apparatus controlling device 30, this ID code will be recorded on the memory 32a at the time. For this reason, between the security control device 10 and the portable apparatus controlling device 30, two communications like said 2nd embodiment are unnecessary, and require only one communication.

[0094]

Therefore, if it changes in this way, it can add to the effect of the above (5) and the communication mode of the security control system 1 for vehicles at the time of ID

registration control can be simplified rather than a 2nd embodiment.

[0095]

(A 3rd embodiment)

Next, a 3rd embodiment that materialized this invention is described based on drawing 1 and drawing 5.

In addition to the control mode of the security control system 1 for vehicles in said 1st embodiment or said 2nd embodiment, this embodiment performs security release restriction control. That is, in this embodiment, the ID registration control shown by said 1st embodiment or said 2nd embodiment and this security release restriction control are combined, and the security control system 1 for vehicles performs them. Then, the security release restriction control performed by the security control system 1 for vehicles of this embodiment is explained in detail hereafter.

[0096]

If restriction operation is performed by the user in this embodiment as for the cellular phone 4, a restriction requirement signal will be transmitted to the portable apparatus controlling device 30 (refer to drawing 1). The cellular phone 4 judges that restriction operation was performed, when the password for function restrictions which can be set up, for example by a user is inputted from a ten key, and it transmits the restriction requirement signal containing the password cord for function restrictions to the portable apparatus controlling device 30. the password for function restrictions -- when the portable apparatus designation number which specifies both the portable apparatus 3 is inputted from a ten key, the cellular phone 4 transmits the restriction requirement signal containing the password cord for function restrictions, and a portable apparatus designation code to the portable apparatus controlling device 30. Here, with the password cord for function restrictions, it is equivalent to what carried out binary conversion of the password for function restrictions. A portable apparatus designation number shows the registration number of the ID code recorded on the memory 32a of said portable apparatus controlling device 30, and it is equivalent to what carried out binary conversion of this portable apparatus designation number with a portable apparatus designation code.

[0097]

And the portable apparatus controlling device 30 will perform restriction instruction control which transmits a function restriction signal to the security control device 10, if the restriction requirement signal from the cellular phone 4 is received.

In detail, the portable apparatus controlling device 30 receives a restriction requirement signal by the communications department 33 for portable devices. That is, the communications department 33 for portable devices functions as a reception means which receives a restriction requirement signal. For this reason, this restriction requirement signal is inputted into the supervisory control part 32. The supervisory control part 32 will judge the existence of the password cord for function restrictions contained in this restriction requirement signal, and the corresponding password cord for function restrictions from the

password cord for function restrictions already recorded on the memory 32a, if a restriction requirement signal is inputted (password cord existence judgment).

[0098]

The password cord for function restrictions is recorded on the memory 32a at the time of car registration control. It is the control which registers the vehicle information of the vehicles 2 into the portable apparatus controlling device 30 in order to set up the vehicles 2 as an administration object of the portable apparatus controlling device 30, and in said 1st embodiment and a 2nd embodiment, this car registration control is performed similarly. And in this embodiment, at the time of this car registration control, it is transmitted to the portable apparatus controlling device 30 with vehicle information from the security control device 10, and the password cord for function restrictions is recorded on the memory 32a in the state where it matched with this vehicle information. The portable apparatus controlling device 30 will transmit the car registration completion signal which shows that car registration was completed to the security control device 10, if vehicle information and the password cord for function restrictions are recorded on the memory 32a by such car registration control.

[0099]

When the password cord for function restrictions contained in a restriction requirement signal and the corresponding password cord for function restrictions exist in the memory 32a as a result of said password cord existence judgment, the supervisory control part 32 specifies the vehicles 2 used as the administration object of restriction instruction control based on this password cord for function restrictions, and corresponding vehicle information. And the supervisory control part 32 transmits the function restriction signal containing a function restriction code via the management communications department 31 to the security control device 10 carried in the specified vehicles 2 (refer to drawing 1). When said portable apparatus designation code is contained in the restriction requirement signal, the supervisory control part 32 reads the ID code with which the registration number which is in agreement with a portable apparatus designation code among the ID codes recorded on the memory 32a corresponding to vehicle information was matched. And the supervisory control part 32 transmits the function restriction signal containing the read ID code and said function restriction code via the management communications department 31.

[0100]

On the other hand, the security control device 10 will perform function restriction processing which restricts or forbids the drive of the door lock drive device 22 or Engine control section 23 based on communication with the portable apparatus 3 mentioned above, if the function restriction signal transmitted from the portable apparatus controlling device 30 is received.

[0101]

In detail, the security control device 10 receives a function restriction signal by the security communication part 14. For this reason, this function restriction signal is inputted into the

vehicle control part 13. The vehicle control part 13 will judge whether the ID code is contained in this function restriction signal, if a function restriction signal is inputted. As a result, when the ID code is not contained in the function restriction signal, the vehicle control part 13 restricts or forbids control of the door lock drive device 22 or Engine control section 23, even if communication with which portable apparatus 3 which can communicate is materialized. That is, even if communication with the portable apparatus 3 with which the vehicle control part 13 corresponds in this case with all the ID codes currently recorded on the memory 13a is materialized, security release of security equipments (the door lock drive device 22 and Engine control section 23) is restricted or forbidden. Only when communication with the portable apparatus 3 with which the vehicle control part 13 corresponds with this ID code when the ID code is contained in the function restriction signal is materialized, control of the door lock drive device 22 or Engine control section 23 is restricted or forbidden.

[0102]

In this embodiment, the vehicle control part 13 can be set up by a user about which processing of these function restriction processing shown in the following <a> or <b> is performed, and is performed.

[0103]

The <a> 1st function restriction processing (security release prohibition process)

(a-1) When the ID code is not contained in the function restriction signal

In this case, if the ID code signal from the portable apparatus 3 and the lock/unlock command signal from the portable apparatus 3 which were answered and transmitted to the request signal are received, the vehicle control part 13, Though the ID code contained in these ID code signals or a lock/unlock command signal was recorded on the memory 13a, control of the door lock drive device 22 or Engine control section 23 is not performed. That is, the vehicle control part 13 forbids unlocking of a door lock, and engine start up, even if communication with the portable apparatus 3 is materialized. If it puts in another way, and a function restriction signal is inputted, the vehicle control part 13 will forbid security releasing operation called start-up permission of the engine by unlocking and Engine control section 23 of the door lock by the door lock drive device 22.

[0104]

(a-2) When the ID code is contained in the function restriction signal

In this case, the vehicle control part 13 compares first the ID code contained in this ID code signal or a lock/unlock command signal with the ID code contained in a function restriction signal, if the ID code signal from the portable apparatus 3 and the lock/unlock command signal from the portable apparatus 3 which were answered and transmitted to the request signal are received. As a result, the vehicle control part 13 is restricted when these ID codes are in agreement, and it does not perform control of the door lock drive device 22 or Engine control section 23. That is, only when communication with the portable apparatus 3 with which the vehicle control part 13 corresponds with the ID code contained in a function



restriction signal in this case is materialized, unlocking of a door lock and engine start up, i.e., security releasing operation, are forbidden. Therefore, the vehicle control part 13 performs security releasing operation as usual, when the ID code signal and lock/unlock command signal containing other ID codes (ID code which is not contained in the functional limiting signal) recorded on the memory 13a are received. That is, only the security releasing operation using the specific portable apparatus 3 is forbidden here.

[0105]

The <b> 2nd function restriction processing (security release restriction processing)

(b-1) When the ID code is not contained in the function restriction signal

In this case, if the ID code signal from the portable apparatus 3 and the lock/unlock command signal from the portable apparatus 3 which were answered and transmitted to the request signal transmitted to outdoor [ of the vehicles 2 ] are received, the vehicle control part 13 will carry out drive controlling of the door lock drive device 22, and will perform lock/unlock control of a door lock. However, when the ID code signal from the portable apparatus 3 answered and transmitted to the request signal transmitted to the interior of a room of the vehicles 2 is received, the vehicle control part 13 will not be in an engine start authorized state. For this reason, even if a start switch is operated, the vehicle control part 13 will not control Engine control section 23. That is, although the vehicle control part 13 performs lock/unlock of a door lock when communication with the portable apparatus 3 is materialized, it forbids about engine start up. If it puts in another way, and a function restriction signal is inputted, the vehicle control part 13 will restrict security releasing operation.

[0106]

(b-2) When the ID code is contained in the function restriction signal

Also in this case, if the ID code signal from the portable apparatus 3 and the lock/unlock command signal from the portable apparatus 3 which were answered and transmitted to the request signal transmitted to outdoor [ of the vehicles 2 ] are received, the vehicle control part 13 will carry out drive controlling of the door lock drive device 22, and will perform lock/unlock control of a door lock. That is, the vehicle control part 13 performs lock/unlock control of a door lock like the time of the ID code not being contained in the function restriction signal here. However, when the ID code signal from the portable apparatus 3 answered and transmitted to the request signal transmitted to the interior of a room of the vehicles 2 is received after the function restriction signal containing an ID code was inputted. The vehicle control part 13 compares the ID code with which the ID code first contained in this ID code signal is contained in a function restriction signal. As a result, it will restrict, when the ID code contained in an ID code signal is in agreement with the ID code contained in a function restriction signal, and the vehicle control part 13 will not be in an engine start authorized state. That is, although lock/unlock of a door lock is performed when communication with the portable apparatus 3 with which the vehicle control part 13 corresponds with the ID code contained in a function restriction signal in this case is

materialized, it forbids about engine start up. If it puts in another way and the function restriction signal containing an ID code will be inputted, the vehicle control part 13 will restrict only the security releasing operation based on communication with this ID code and the corresponding portable apparatus 3. Therefore, the vehicle control part 13 performs security releasing operation as usual, when the ID code signal and lock/unlock command signal containing other ID codes (ID code which is not contained in the functional limiting signal) recorded on the memory 13a are received. That is, only the security releasing operation using the specific portable apparatus 3 is restricted here.

[0107]

When the restriction release signal which shows that restriction control is canceled is inputted, the vehicle control part 13 cancels such function restriction control, and switches to the usual security control mode. For this reason, if input into the cellular phone 4 the restriction release number which turns into a restriction release signal, for example, communication between the cellular phone 4, the portable apparatus controlling device 30, and the security control device 10 is made to perform and the security control device 10 is made to receive this restriction release signal, it will switch to the usual security control mode.

[0108]

By the way, the security control device 10 will switch to car registration mode, if predetermined operation is performed. If the car registration shift switch which was formed, for example in the vehicles 2 and which is not illustrated is specifically operated, the signal (car registration shift signal) which shows the purport of the operation will be inputted into the vehicle control part 13. And if this car registration shift signal is inputted, the vehicle control part 13 will switch to car registration mode, and will transmit a car registration signal including vehicle information to the portable apparatus controlling device 30 via the security communication part 14. The input signal from the input device (for example, input parts, such as a car-navigation system) which is not illustrated can be inputted into the vehicle control part 13. And if the password for function restrictions which can be set up by a user is inputted into this input device and the input signal which consists of this password for function restrictions is inputted into the vehicle control part 13 after switching to car registration mode, The vehicle control part 13 transmits the car registration signal containing vehicle information and the password cord for function restrictions to the portable apparatus controlling device 30 via the security communication part 14. For this reason, where the vehicle information and the password cord for function restrictions of the vehicles 2 are matched, it is recorded on the memory 32a of the portable apparatus controlling device 30.

[0109]

If the car registration completion signal transmitted from the portable apparatus controlling device 30 is inputted into the vehicle control part 13 via the security communication part 14, this vehicle control part 13 will perform the display which shows that registration of the

vehicles 2 was completed to the indicator which was formed in the interior of a room of the vehicles 2, and which is not illustrated.

[0110]

Next, the communication mode at the time of the car registration control which registers the vehicle information of the vehicles 2 into the portable apparatus controlling device 30, and sets up the vehicles 2 as an administration object of the portable apparatus controlling device 30 in the security control system 1 for vehicles of this embodiment, The communication mode at the time of function restriction control is explained using the sequence chart shown in drawing 5.

[0111]

<The communication mode at the time of car registration control>

As shown in the figure, registration of the vehicles 2 to the portable apparatus controlling device 30 is performed by communication between the security control device 10 and the portable apparatus controlling device 30.

[0112]

In detail, first, the security control device 10 will switch to car registration mode, if transition operation to car registration mode is performed (Step S61). Here, if the password for function restrictions is inputted from said input device (Step S62), the security control device 10 will transmit the car registration signal containing the vehicle information and the password cord for function restrictions of the vehicles 2 to the portable apparatus controlling device 30 (Step S63).

[0113]

If the car registration signal from the security control device 10 is received, the portable apparatus controlling device 30 will record the vehicle information and the password cord for function restrictions which are contained in this car registration signal on the memory 32a, and will complete registration (administrative vehicle registration) of the vehicles 2 used as an administration object (Step S64). For this reason, the security control device 10 (vehicles 2) is registered into the portable apparatus controlling device 30 as an administration object. And the portable apparatus controlling device 30 transmits the car registration completion signal which shows that car registration was completed to the security control device 10 (Step S65).

[0114]

The security control device 10 will notify the purport of registration completion by displaying on an indicator that registration of the vehicles 2 was completed, if the car registration completion signal from the portable apparatus controlling device 30 is received (Step S66). For this reason, recognition of a user is certainly attained [ that registration of the vehicles 2 was completed, and ] by recognizing this indicator visually.

[0115]

<The communication mode at the time of function restriction control>

As shown in the figure, function restriction control is performed by communication between

the security control device 10, the portable apparatus controlling device 30, and the cellular phone 4.

[0116]

In detail, first, the cellular phone 4 will transmit said restriction requirement signal containing the password cord for function restrictions to the portable apparatus controlling device 30, if said restriction operation is performed and the password for function restrictions is inputted (Step S71) (Step S72). Here, the cellular phone 4 transmits the restriction requirement signal containing the password cord for function restrictions, and a portable apparatus designation code to the portable apparatus controlling device 30, when a portable apparatus designation number is inputted with the password for function restrictions.

[0117]

The portable apparatus controlling device 30 specifies the corresponding vehicles 2 based on the password cord for function restrictions contained in this restriction requirement signal, if a restriction requirement signal is inputted (Step S73). And the portable apparatus controlling device 30 transmits said function restriction signal containing a function restriction code to the security control device 10 formed in the specified vehicles 2 (Step S74). Here, the portable apparatus controlling device 30 transmits the function restriction signal containing this portable apparatus designation code, a corresponding ID code, and a function restriction code, when the restriction requirement signal containing a portable apparatus designation code is inputted.

[0118]

The security control device 10 will perform function restriction processing shown in the above <a> or <b>, if a function restriction signal is inputted from the portable apparatus controlling device 30 (Step S75).

Therefore, according to this embodiment, the following effects can be acquired.

[0119]

(7) If the restriction requirement signal transmitted from the portable transmitter machine (cellular phone 4) which a user possesses is received by the portable apparatus controlling device 30, a function restriction signal will be transmitted from the portable apparatus controlling device 30 to the security control device 10. The security control device 10 forbids or restricts control of the door lock drive device 22 or Engine control section 23, on condition that the function restriction signal was received. That is, the security control device 10 forbids or restricts the security releasing operation by security equipments on condition of reception of this function restriction signal. For this reason, when a user loses the portable apparatus 3 or a theft is carried out, the security releasing operation by the security control device 10 can be forbidden or restricted by making a restriction requirement signal transmit from the cellular phone 4. Therefore, also in the time of loss and the theft of the portable apparatus 3, the security releasing operation by this portable apparatus 3 can be forbidden or restricted immediately, and the high security level of security equipments can be secured.

[0120]

(8) Since the security releasing operation using this portable apparatus 3 will be simply forbidden or restricted by the user even if a third party does the theft of the portable apparatus 3, worth of portable apparatus 3 after a theft falls substantially. Even mind that a third party is going to do the theft of the portable apparatus 3 stops therefore, boiling. That is, the volition of the theft of the portable apparatus 3 by a third party itself can be made to decline, and the anti-theft nature of the portable apparatus 3 also improves.

[0121]

(9) If the portable apparatus designation number which specifies the portable apparatus 3 is inputted by the user when the cellular phone 4 performs restriction operation, the security control device 10 will forbid or restrict only the security release based on communication with the this specified portable apparatus 3. That is, if the portable apparatus 3 which should be restricted is specified when the cellular phone 4 performs restriction operation, only the security release by the specific portable apparatus 3 can be made to forbid or restrict. For this reason, when the portable apparatus 3 is lost, for example or a theft is carried out, only the security release by that portable apparatus 3 can be forbidden or restricted, and a passage becomes usually possible about the security release by the portable apparatus 3 registered into others. That is, about the portable apparatus 3 by which is lost or a theft is not carried out, it becomes available, without receiving restriction in any way. Therefore, even the security release by the portable apparatus 3 which does not need function restriction cannot be forbidden or restricted, and the convenience of the portable apparatus 3 can be secured.

[0122]

The embodiment of this invention may be changed as follows.

- The mutual recognition (pairing) for judging whether each is operating normally between the vehicle control part 13 of the security control device 10 and the security communication part 14 may be made to perform in said 1st embodiment. And when it is judged that each is operating normally (i.e., only when this mutual recognition is materialized), it is good also as registration to the security control device 10 being possible in the ID code of the portable apparatus 3. Since the mutual recognition between both will not be materialized when the security communication part 14 is removed unjustly or is destroyed, for example if it does in this way, it cannot register with the security control device 10. Therefore, unjust registration of an ID code can be prevented more certainly.

[0123]

- A GPS module is provided in the portable apparatus 3, the position of the portable apparatus 3 is recognized with the portable apparatus controlling device 30 at the time of function restriction, and it may be made to notify the position of this portable apparatus 3 to the cellular phone 4 from the portable apparatus controlling device 30 in a 3rd embodiment. If it does in this way, the user can recognize certainly the whereabouts of the portable apparatus 3 by which was lost or the theft was carried out.

[0124]

- According to a 3rd embodiment, a restriction requirement signal is transmitted from the cellular phone 4 to the portable apparatus controlling device 30. However, restriction operation by a user is enabled by the vehicles 2, and it is good from the security control device 10 also considering a restriction requirement signal as ability ready for sending to the portable apparatus controlling device 30. That is, it is good by performing restriction operation by the vehicles 2 also as possible in the function restriction of security equipments (the door lock drive device 22 and Engine control section 23). If it does in this way, when performing function restriction, portable transmitter machines, such as the cellular phone 4, become unnecessary.

[0125]

- When the function restriction signal which the vehicle control part 13 is in the state set as said security release prohibition process, and does not contain an ID code is inputted in a 3rd embodiment, it may be changed so that the output of the request signal to the sending circuit 11 at the time of security control mode may be forbidden. If it changes in this way and a function restriction signal will be inputted into the vehicle control part 13, communication with the security control device 10 and the portable apparatus 3 in security control mode will become impossible. Therefore, communication with the portable apparatus 3 and the vehicle control part 13 stops materializing, and control of the door lock drive device 22 by the vehicle control part 13 and Engine control section 23 is forbidden. Therefore, the useless communication between the portable apparatus 3 and the security control device 10 can be prevented, and the power consumption of the portable apparatus 3 and the security control device 10 can be reduced.

[0126]

- In a 3rd embodiment of the above, the portable apparatus controlling device 30 transmits a function restriction signal to the security control device 10. However, the portable apparatus controlling device 30 transmits a function restriction signal to the portable apparatus 3 (portable apparatus 3 which has the ID code matched with the password cord for function restrictions) used as a function restriction object. In this case, the portable apparatus 3 is constituted so that the portable apparatus controlling device 30 and communication are possible. When the function restriction signal from the portable apparatus controlling device 30 is received, the portable apparatus 3 is constituted so that it may become impossible transmitting an ID code signal and a lock/unlock command signal. Even if it does in this way, the security releasing operation using the portable apparatus 3 by which function restriction was carried out can become impossible, and the security level of security equipments can be raised further.

[0127]

- Make a car registration signal transmit to the portable apparatus controlling device 30 from the security control device 10 in each aforementioned embodiment at the time of the car registration control for setting up the vehicles 2 as an administration object of the

portable apparatus controlling device 30. However, at the time of such car registration control, the security control device 10 is good for the portable apparatus controlling device 30 also considering said car registration signal as ability ready for sending from the registration device formed independently. For example, it is good for the portable apparatus controlling device 30 also considering a car registration signal as ability ready for sending from this personal computer, using a personal computer as a registration device. In this case, car registration information, including vehicle information, the password for function restrictions, etc., is inputted into a personal computer, and it is made to make a car registration signal including this car registration information transmit to the portable apparatus controlling device 30 via communications networks, such as the Internet. Since it will necessarily be [ the security control device 10 (vehicles 2) ] less necessary for car registration work if it does in this way, the convenience of this car registration work improves. If the password set up by the user, the dealer, the maker of the portable apparatus 3, etc. is given to a car registration signal, the unjust car registration by a third party can be prevented.

[0128]

the ID code of the portable apparatus 3 which can be registered into a car registration signal at the security control device 10 -- one sort -- or two or more sorts may be contained. In this case, when the portable apparatus controlling device 30 receives this car registration signal, it is made to record on the memory 32a in the state where matched with vehicle information and it carried out, by making the ID code contained in that signal into the ID code which can be registered. And when the portable apparatus controlling device 30 receives the registered signal and registration permission requirement signal which are transmitted from the security control device 10, It is made to judge to this portable apparatus controlling device 30 based on whether to be in agreement with the ID code with which the ID code contained in this registered signal or a registration permission requirement signal is already recorded on the memory 32a and which can be registered whether registration of an ID code is appropriate. That is, the portable apparatus controlling device 30 will recognize only the ID code which was acquired at the time of car registration control and which can be registered in this case as an ID code which can be registered into the security control device 10. If it does in this way, even if a third party is going to register unjustly into the security control device 10 the portable apparatus 3 which does not have an ID code which can be registered, this registration will be judged not to be appropriate by the portable apparatus controlling device 30, and that will be notified to the cellular phone 4. That is, registration to the security control device 10 only of the portable apparatus 3 which has the ID code set up as an ID code which can be registered is attained. Therefore, unjust registration of the ID code by a third party can be deterred, and the security level of security equipments can be raised further.

[0129]

The work (car registration work) which registers the vehicles 2 into the portable apparatus

controlling device 30 and the work (ID registration work) which registers the ID code of the portable apparatus 3 into the security control device 10, It is carried out by workers who can trust it for a user, such as not only a user but a dealer, and a maker of the portable apparatus 3.

[0130]

- The security control system 1 for vehicles does not perform ID registration control shown by said 1st embodiment or said 2nd embodiment, but performs only security release restriction control shown by said 3rd embodiment.

[0131]

- In each aforementioned embodiment, the wire communication for which the communication between the security control device 10 and the portable apparatus controlling device 30 used the public network in addition to radio, for example may be adopted. For example, the end connection to which the modular jack of a telephone is connected is provided in the vehicles 2, and it may be made to perform communication with the security control device 10 and the portable apparatus controlling device 30 using a telephone wire.

[0132]

- Not only the cellular phone 4 but in each aforementioned embodiment, portable transmitter machines may be a personal computer of a note type, PDA (Personal Digital Assistance : Personal Digital Assistant), communication equipment for exclusive use, etc., for example.

[0133]

- The security control system 1 for vehicles of each aforementioned embodiment is provided with the following.

The function in which a door lock is automatically unlocked by the two-way communication of the portable apparatus 3 and the security control device 10 because the portable apparatus 3 approaches the vehicles 2 (smart entry function).

The function in which engine start up is permitted because the portable apparatus 3 advances into the interior of a room of the vehicles 2 (smart ignition function).

However, the security control system 1 for vehicles does not need to be provided with such a smart entry function or smart ignition function. For example, when the portable apparatus 3 is provided with a transponder and a machinery key and equips the vehicles 2 with this machinery key, it performs two-way communication with the security control device 10. And on condition that rotating operation of this machinery key was carried out, it controls the door lock drive device 22 and Engine control section 23, while permitting the rotating operation of a machinery key, when the security control device 10 is materialized [ two-way communication with this transponder ]. That is, the security control device 10 should just perform security releasing operation based on two-way communication with the portable apparatus 3.

[0134]



It may not be indispensable about the two-way communication of such the portable apparatus 3 and the security control device 10, either. For example, it may be ability ready for sending only about said lock/unlock command signal, and the security control device 10 is not provided with the sending circuit 11 with it, but the portable apparatus 3 may be constituted so that a request signal may not be transmitted. That is, if the security control device 10 is coming to perform security releasing operation based on the sending signal containing the ID code transmitted from the portable apparatus 3, two-way communication with the portable apparatus 3 will not necessarily be performed.

[0135]

- In each aforementioned embodiment, the portable apparatus controlling device 30 manages the number of the ID codes of the portable apparatus 3 which can be registered into the security control device 10 formed in the vehicles 2 used as an administration object. However, the portable apparatus controlling device 30 does not necessarily manage the number of these ID codes.

[0136]

- If the security control system 1 for vehicles switches even the security control device 10 to ID registration mode in each aforementioned embodiment, registration of the portable apparatus 3 is possible anywhere. However, a GPS module is connected to the security control device 10, for example, The security control system 1 for vehicles may be changed so that the registration of the portable apparatus 3 of the security control device 10 may be attained only at the predetermined places (for example, a house, a company, a dealer, etc.) set up beforehand. If it does in this way, unjust registration of the ID code by a third party can be prevented further, and the security level of security equipments can be raised further.

[0137]

- In each aforementioned embodiment, the operation for switching the security control device 10 to ID registration mode is not limited to operation of the mode switch 21. For example, the existing switches (for example, lever combination switch etc.) with which the security control device 10 was formed in the vehicles 2, It may be changed so that it may switch to ID registration mode in a predetermined mode (presetting by the user or a dealer of the mode which only a user and a dealer can know, etc. are desirable). If it does in this way, the mode switch 21 is omissible. A change in the ID registration mode which is not meant can be prevented by the operation mistake of the mode switch 21.

[0138]

- The aforementioned portable apparatus controlling device 30 may be allocated in not only a control center for exclusive use but a user's house, etc., and may be constituted by the personal computer etc. in this case.

- In said each embodiment, the cellular phone 4 transmits registration yes-or-no information and a restriction requirement signal to the portable apparatus controlling device 30, when voice input of the predetermined voice commanding is carried out.

[0139]

Communication between the cellular phone 4 and the portable apparatus controlling device 30 may be performed by the conversation of the operator and user who are residing at the control center in which the portable apparatus controlling device 30 was allocated. That is, a user telephones a control center using the cellular phone 4, and directs registration yes or no and a restriction demand by conversation with an operator. In this case, the operator which received directions will operate the portable apparatus controlling device 30 based on these directions, and will perform registration restriction control and function restriction control. If it does in this way, it will become unnecessary to make registration yes-or-no information and a restriction requirement signal transmit to the portable apparatus controlling device 30 from the cellular phone 4.

[0140]

- The door lock drive device 22 or not only Engine control section 23 but security equipments may be a steering lock device, a shift lock device, a tire locking device, etc., for example. That is, if it is a device for restricting or checking a run of the normal vehicles 2, it is applicable as security equipments.

[0141]

- A security control system may be materialized as a security system for buildings which controls the lock/unlock of the door for buildings, for example in addition to the security control system 1 for vehicles which controls the security equipments of vehicles.

[0142]

Next, the technical ideas grasped by the embodiment mentioned above are enumerated below besides the technical idea indicated to the claim.

(1) In the security control system according to claim 3, when you judge that registration of said ID code is not appropriate to said portable apparatus controlling device, perform report control which notifies the unusual reporting signal which shows that to the portable transmitter machine which a user possesses. According to the invention given in this technical idea (1), the user can recognize certainly and promptly that the ID code of portable apparatus tended to be registered unjustly through a portable transmitter machine.

[0143]

(2) In the security control system of a statement, in claims 2-4 and any 1 paragraph of a technical idea (1) said portable apparatus controlling device, Judge whether registration of the ID code contained in said registered signal is appropriate based on the registration yes-or-no information transmitted from the portable transmitter machine which a user possesses. According to the invention given in this technical idea (2), the registration propriety of an ID code can be freely set up by a user.

[0144]

(3) In the security control system of a statement, in any 1 paragraph of claims 1-4, a technical idea (1), and (2) said security control device, Perform mutual recognition of

whether each is operating normally said security communication means, said control means, and in between, only when this mutual recognition is materialized, register an ID code, and when this mutual recognition is not materialized, forbid registration of an ID code. According to the invention given in this technical idea (3), since registration of an ID code is forbidden when a security communication means is removed, for example or it is destroyed, unjust registration of an ID code can be prevented more certainly.

[0145]

(4) To claims 1-4 and technical idea (1) - (3), in the security control system of a statement, said security control device is an object for vehicles, and said security equipments, At least one side of the Engine control sections which control the start-up permission of a door lock drive device and an engine which controls the lock/unlock of a door lock should be included.

[0146]

(5) In the security control method according to claim 12 at the time of said ID registration control. When a registration permission requirement signal is transmitted to said portable apparatus controlling device from said security control device and this portable apparatus controlling device receives this registration permission requirement signal, with this portable apparatus controlling device. While judging whether registration of said ID code is appropriate, the reply signal which shows the decision result is transmitted to said security control device, On condition that said security control device received said reply signal including the purport that registration of said ID code is appropriate, record this ID code on said recording device, and complete registration of an ID code.

[Brief Description of the Drawings]

[0147]

[Drawing 1]The block diagram showing the 1st which materialized this invention to the security control system for vehicles - the outline composition of a 3rd embodiment.

[Drawing 2]The sequence chart which shows the communication mode of a 1st embodiment.

[Drawing 3]The sequence chart which shows the communication mode of a 2nd embodiment.

[Drawing 4]The sequence chart which shows the example of change of the communication mode of a 2nd embodiment.

[Drawing 5]The sequence chart which shows the communication mode of a 3rd embodiment.

[Description of Notations]

[0148]

1 [ -- The cellular phone as a portable transmitter machine, ] -- The security control system for vehicles, 2 -- Vehicles, 3 -- Portable apparatus, 4 10 -- A security control device, 13 -- The vehicle control part as a control means, 13a -- The memory as a recording device, 14 - - The security communication part as a security communication means, 22 [ -- The

management communications department, 32 / -- The supervisory control part as a management tool 33 / -- The communications department for portable devices as the means of communication for portable devices, and a reception means. ] -- The door lock drive device as security equipments, 23 -- The Engine control section as security equipments, 30 -- A portable apparatus controlling device, 31

---

[Translation done.]

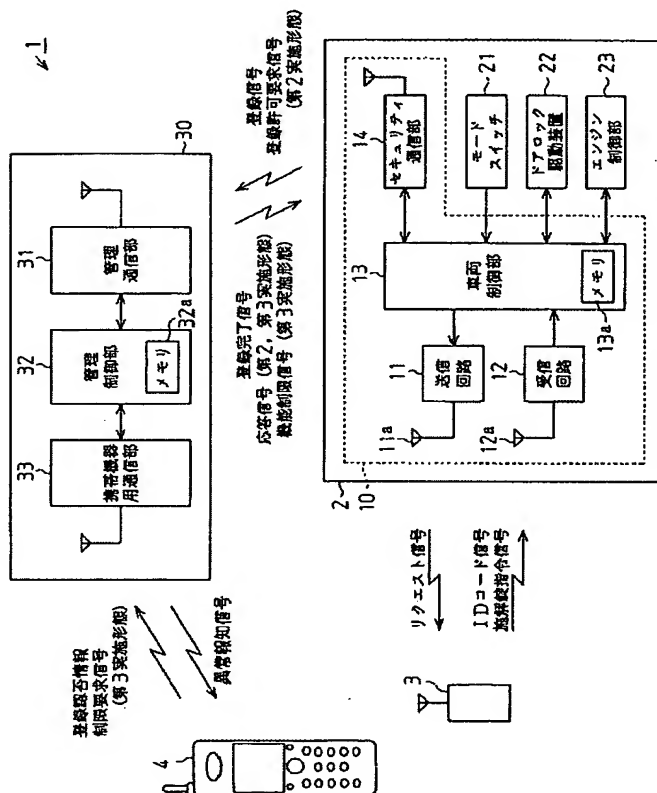
\* NOTICES \*

JPO and INPIT are not responsible for any  
damages caused by the use of this translation.

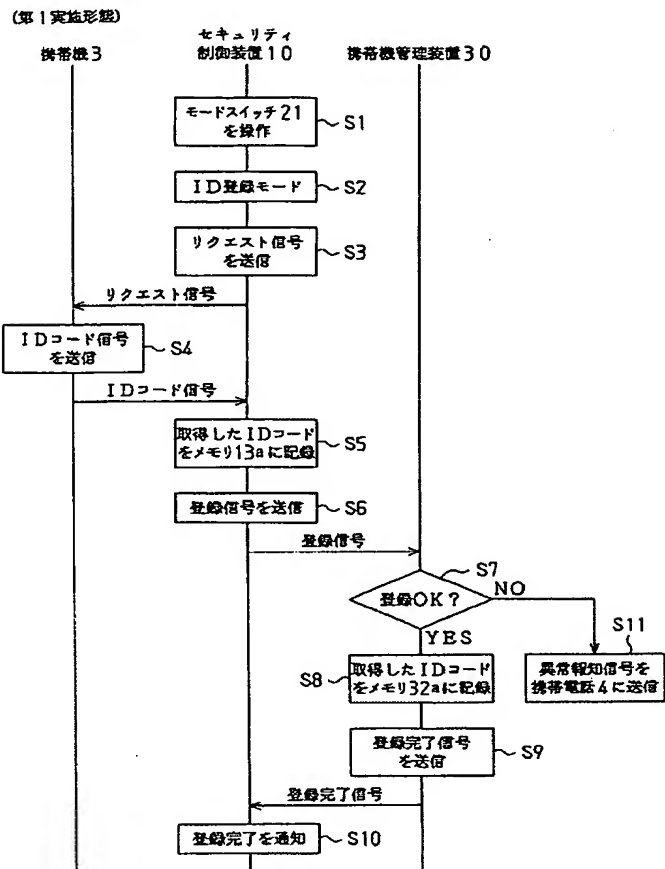
- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.\*\*\*\* shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

## DRAWINGS

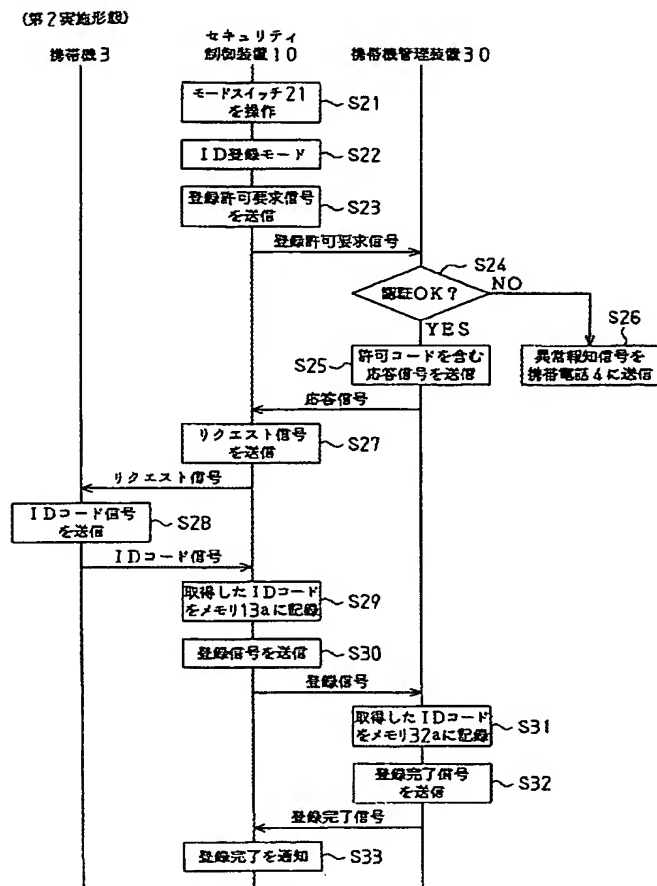
[Drawing 1]



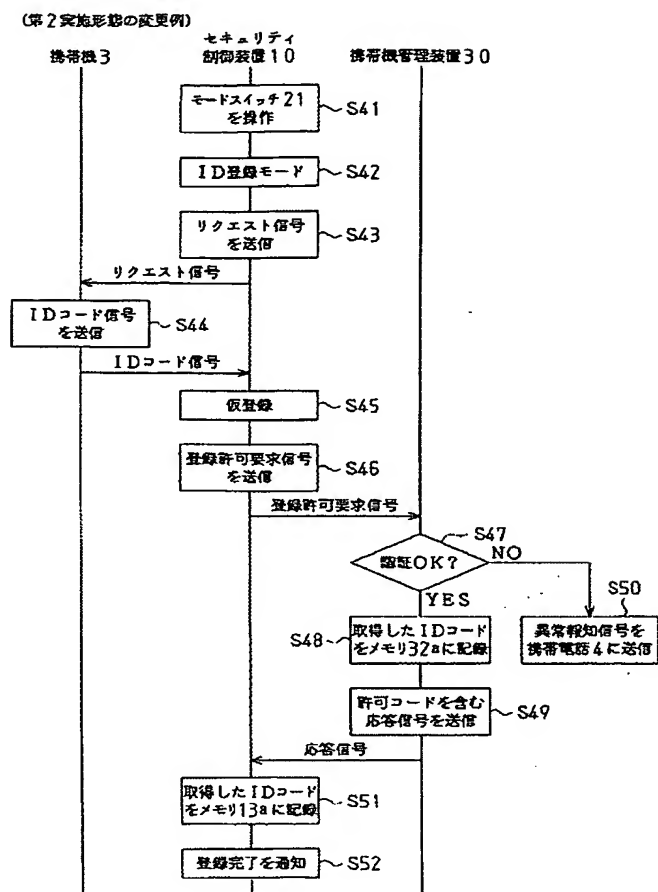
[Drawing 2]



[Drawing 3]



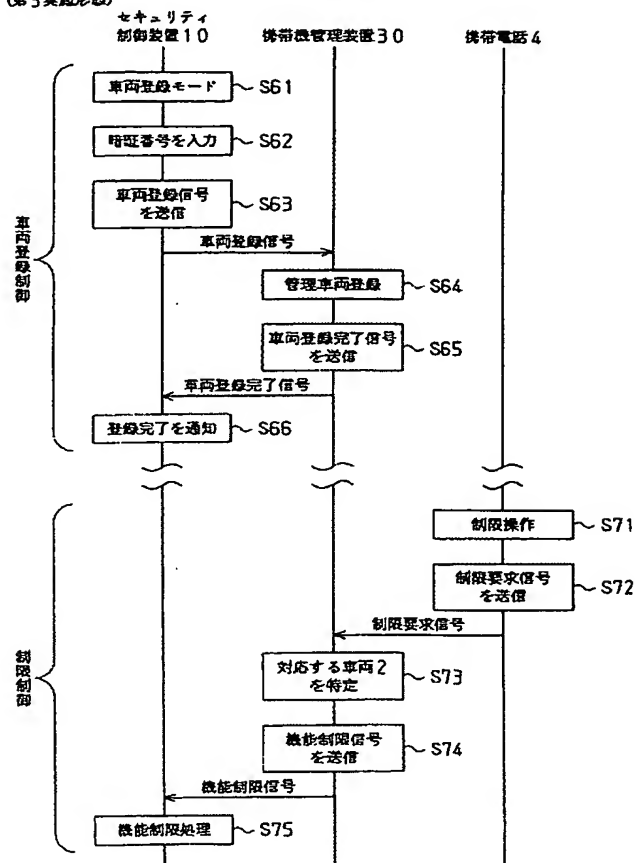
[Drawing 4]



[Drawing 5]



(第3実施形態)



[Translation done.]

(19) 日本国特許庁 (JP)

## (12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2005-226389

(P2005-226389A)

(43) 公開日 平成17年8月25日 (2005.8.25)

(51) Int. Cl.<sup>7</sup>

E05B 49/00  
B60R 25/00  
B60R 25/04

F1

E05B 49/00 K  
B60R 25/00 606  
B60R 25/04 608

テーマコード (参考)

2E250

審査請求 未請求 請求項の数 12 O L (全 29 頁)

(21) 出願番号 特願2004-38022 (P2004-38022)  
(22) 出願日 平成16年2月16日 (2004.2.16)

(71) 出願人 000003551  
株式会社東海理化電機製作所  
愛知県丹羽郡大口町豊田三丁目260番地  
(71) 出願人 000003207  
トヨタ自動車株式会社  
愛知県豊田市トヨタ町1番地  
(74) 代理人 100068755  
弁理士 恩田 博宣  
(74) 代理人 100105957  
弁理士 恩田 誠  
(72) 発明者 河村 大輔  
愛知県丹羽郡大口町豊田三丁目260番地  
株式会社東海理化電機製作所内

最終頁に続く

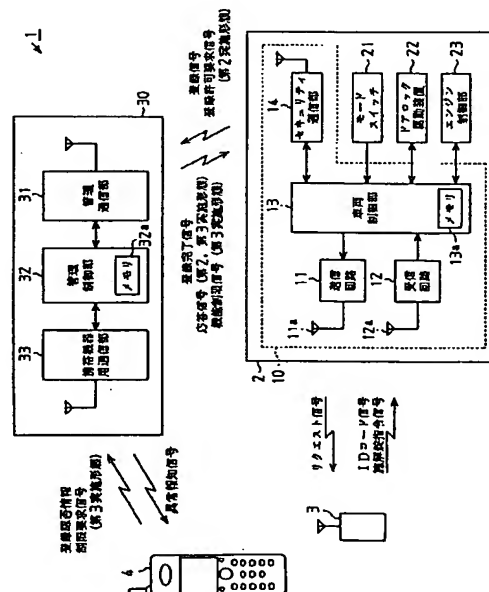
(54) 【発明の名称】 セキュリティ制御システム、セキュリティ制御装置、携帯機管理装置、及び、セキュリティ制御方法

## (57) 【要約】

【課題】 セキュリティ機器のセキュリティレベルをより一層向上させることができるセキュリティ制御システム、セキュリティ制御装置、携帯機管理装置、及び、セキュリティ制御方法を提供する。

【解決手段】 セキュリティ制御装置10は、携帯機3との通信により、携帯機3に設定されたIDコードとメモリ13aに既に記録されているIDコードとの照合を行い、該照合の成立の有無に基づいてドアロック駆動装置22やエンジン制御部23を制御する。また、セキュリティ制御装置10は、携帯機3に設定されたIDコードをメモリ13aに記録するID登録制御を行い、該ID登録制御時にあっては、登録対象となるIDコードを含む登録信号を携帯機管理装置30に送信する。携帯機管理装置30は、セキュリティ制御装置10からの登録信号を受信し、該登録信号に含まれるIDコードに基づいて、対応する携帯機3の管理を行う。

【選択図】 図1



## 【特許請求の範囲】

## 【請求項 1】

通信機能を有する携帯機との通信により、携帯機に設定された I D コードと自身の記録手段に既に記録されている I D コードとの照合を行い、該照合の成立の有無に基づいてセキュリティ機器を制御するセキュリティ制御装置と、該セキュリティ制御装置との通信を行うことにより、対応する前記携帯機の管理を行う携帯機管理装置とを備えたセキュリティ制御システムであって、

前記セキュリティ制御装置は、前記携帯機に設定された I D コードを前記記録手段に記録する I D 登録制御を行い、該 I D 登録制御時にあっては、登録対象となる I D コードを含む登録信号を前記携帯機管理装置に送信し、

10

該携帯機管理装置は、前記登録信号に基づいて、対応する携帯機の管理を行うことを特徴とするセキュリティ制御システム。

## 【請求項 2】

前記セキュリティ制御装置は、前記 I D 登録制御時にあっては、登録を完了した I D コードを含む前記登録信号を前記携帯機管理装置に送信し、

前記携帯機管理装置は、前記登録信号を受信した際に、該登録信号に含まれる I D コードの登録が妥当か否かの判断を行い、該登録が妥当ではないと判断した際に、異常登録がなされた旨を示す異常報知信号を、ユーザが所持する携帯通信機器に通報する通報制御を行うことを特徴とする請求項 1 に記載のセキュリティ制御システム。

20

## 【請求項 3】

前記セキュリティ制御装置は、前記 I D 登録制御時にあっては、登録許可要求信号を前記携帯機管理装置に送信し、

前記携帯機管理装置は、前記登録許可要求信号を受信した際に、前記 I D コードの登録が妥当か否かの判断を行うとともに、その判断結果を示す応答信号を前記セキュリティ制御装置に送信し、

前記セキュリティ制御装置は、前記 I D コードの登録が妥当である旨を含む前記応答信号を受信したことを条件として、該 I D コードを前記記録手段に記録することを特徴とする請求項 1 に記載のセキュリティ制御システム。

## 【請求項 4】

前記携帯機管理装置は、ユーザが所持する携帯通信機器から送信される制限要求信号を受信する受信手段を備え、該受信手段により該制限要求信号を受信したことを条件として前記セキュリティ制御装置に機能制限信号を送信し、

30

前記セキュリティ制御装置は、前記機能制限信号を受信したことを条件として、前記セキュリティ機器によるセキュリティ解除動作を禁止または制限することを特徴とする請求項 1 ～ 3 のいずれか 1 項に記載のセキュリティ制御システム。

## 【請求項 5】

固有の I D コードが設定された携帯機との通信を行う携帯機用通信手段と、前記 I D コードと対応する I D コードが記録される記録手段と、前記携帯機との通信時に、携帯機に設定された I D コードと前記記録手段に記録された I D コードとの照合を行い、該照合が一致したか否かに基づいてセキュリティ機器を制御するセキュリティ制御手段とを備えるセキュリティ制御装置であって、

40

当該セキュリティ制御装置の外部に配設されるとともに、前記記録手段に記録された I D コードに基づいて前記携帯機の管理を行う携帯機管理装置と通信可能なセキュリティ通信手段と、

前記携帯機の I D コードを前記記録手段に記録する I D 登録制御を行うとともに、その I D 登録制御の際に、該記録対象となる I D コードを含む登録信号を、前記セキュリティ通信手段を介して前記携帯機管理装置に送信する登録通信制御を行う登録制御手段とを備えることを特徴とするセキュリティ制御装置。

## 【請求項 6】

前記登録制御手段は、前記 I D 登録制御時に、前記セキュリティ通信手段から前記携帯

50

機管理装置に登録許可要求信号を送信する一方、該登録許可要求信号に応答して送信された前記携帯機管理装置からの応答信号が前記セキュリティ通信手段によって受信され、その応答信号に登録許可の旨が含まれていることを条件として、前記IDコードを前記記録手段に登録することを特徴とする請求項5に記載のセキュリティ制御装置。

【請求項7】

前記セキュリティ制御手段は、前記携帯機管理装置から送信される機能制限信号が前記セキュリティ通信手段によって受信されたことを条件として、前記セキュリティ機器によるセキュリティ解除動作を禁止または制限することを特徴とする請求項5または請求項6に記載のセキュリティ制御装置。

【請求項8】

通信機能を有する携帯機との通信に基づき、該携帯機に設定されたIDコードと自身に予め登録されたIDコードとの照合結果に基づいてセキュリティ機器を制御するとともに、前記IDコードの登録時に該IDコードを含む登録信号を外部に送信するセキュリティ制御装置と通信可能な管理通信手段と、

前記登録信号を前記管理通信手段により受信した際に、該登録信号に含まれるIDコードに基づいて該携帯機の管理を行う管理手段とを備えることを特徴とする携帯機管理装置。

【請求項9】

ユーザによって所持される携帯通信機器との通信を行う携帯機器用通信手段を備え、

前記管理手段は、前記管理通信手段によって前記登録信号を受信した際に該登録信号に含まれるIDコードの登録が妥当か否かの判断を行い、該登録が妥当ではないと判断した際に、異常登録がなされた旨を示す異常報知信号を、前記携帯機器用通信手段から前記携帯機器に送信させる異常報知制御を行うことを特徴とする請求項8に記載の携帯機管理装置。

【請求項10】

前記管理手段は、前記携帯機のIDコードの登録時に前記セキュリティ制御装置から送信される登録許可要求信号を前記管理通信手段によって受信した際に、前記IDコードの登録が妥当か否かの判断を行うとともに、その判断結果を示す応答信号を前記セキュリティ制御装置に送信することを特徴とする請求項8に記載の携帯機管理装置。

【請求項11】

ユーザが所持する携帯通信機器から送信される制限要求信号を受信する受信手段を備え、

前記管理手段は、前記受信手段により前記制限要求信号を受信したことを条件として、前記セキュリティ機器によるセキュリティ解除動作を禁止または制限させるための機能制限信号を、前記セキュリティ制御装置及び前記携帯機のうちの少なくとも一方に送信することを特徴とする請求項8～請求項10に記載の携帯機管理装置。

【請求項12】

通信機能を有する携帯機との通信により、携帯機に設定されたIDコードと自身の記録手段に既に記録されているIDコードとの照合を行い、該照合の成立の有無に基づいてセキュリティ機器を制御するセキュリティ制御装置と、該セキュリティ制御装置との通信を行うことにより前記携帯機の管理を行う携帯機管理装置とを備えたセキュリティ制御システムにおけるセキュリティ制御方法であって、

前記携帯機に設定されたIDコードを前記記録手段に登録するID登録制御を前記セキュリティ制御装置により行い、該ID登録制御時に、登録対象となるIDコードを含む登録信号を該セキュリティ制御装置から前記携帯機管理装置に送信し、

前記登録信号に含まれるIDコードと対応する携帯機の管理を、前記携帯機管理装置によって行うことを特徴とするセキュリティ制御方法。

【発明の詳細な説明】

【技術分野】

【0001】

10

20

30

40

50

本発明は、例えば車両や住宅などに用いられるセキュリティ制御システム、セキュリティ制御装置、携帯機管理装置、及び、セキュリティ制御方法に関するものである。

【背景技術】

【0002】

一般に、車両や住宅のドア錠装置などのセキュリティ機器は、ユーザによって所持される専用の機械キーを用いて操作可能となっている。しかし、この場合、機械キーが不正にコピーされたり、ピッキングなどが行われたりすることにより、セキュリティ機器が不正に操作されてしまうおそれがあるため、社会的に問題視されている。

【0003】

そこで従来、セキュリティ機器のセキュリティレベルの向上を図るために、例えば電子照合を用いたセキュリティ制御システムが提案されている（例えば、特許文献1、特許文献2参照）。

【0004】

これら特許文献1、2に示されるように、例えば車両用セキュリティ制御システムでは、ユーザによって所持される携帯機と、車両に配設されたセキュリティ制御装置との間で無線通信が行われる。具体的には、携帯機に設定された固有のIDコードを含むIDコード信号が携帯機からセキュリティ制御装置に送信されると、セキュリティ制御装置は、該IDコード信号に含まれるIDコードと、自身に予め登録されているIDコードとの比較を行う。そして、セキュリティ制御装置は、それらIDコード同士が一致した際に携帯機との通信が成立したと判断し、ドア錠を解錠させたりエンジンの始動許可を行ったりするようになっている。すなわち、セキュリティ制御装置は、携帯機との通信が成立したことを条件として、各種セキュリティ機器のセキュリティ解除動作を行うようになっている。このため、対応する携帯機を所持しない第三者によるセキュリティ解除動作が不能となり、セキュリティ機器のセキュリティレベルが向上する。

【特許文献1】特開2001-289142号公報

【特許文献2】特開2001-311333号公報

【発明の開示】

【発明が解決しようとする課題】

【0005】

ところで、こうした車両用セキュリティ制御システムにおいては、車両制御装置に携帯機のIDコードを予め登録しておくことにより、上述した携帯機と車両制御装置との通信が成立する。このため、例えばスペアキーとしての携帯機を追加登録する場合には、該携帯機のIDコードを登録するID登録操作が必要となる。一般に、このID登録操作を行うためには、所定の操作を行うことによって車両制御装置をID登録モードに切り換え、該ID登録モードにおいて携帯機と車両制御装置との通信を行う必要がある。そして、従来、ディーラーなどでID登録操作が行われるようになっており、特定の作業者のみがID登録モードに切り換えるための操作手順を知り得ようになっている。

【0006】

しかしながら、従来の車両用セキュリティ制御装置では、通常の使用状態においては優れた盗難防止効果を得ることができるものの、携帯機のID登録操作の作業手順を知ってさえいれば、携帯機の不正なID登録が可能となってしまう。このように、従来の車両用セキュリティ制御システムにおいては、特殊なケースではあるものの、万全の盗難防止効果が得られない場合がある。

【0007】

また、IDコードの登録を完了した携帯機をユーザが紛失したり、該携帯機を盗難されたりした場合には、第三者によって該携帯機が使用されてしまうおそれがある。

そこで従来では、セキュリティ機器のセキュリティレベルをより一層高くすることが要望されている。

【0008】

本発明はこうした実情に鑑みてなされたものであり、その目的は、セキュリティ機器の

10

20

30

40

50

セキュリティレベルをより一層向上させることができるセキュリティ制御システム、セキュリティ制御装置、携帯機管理装置、及び、セキュリティ制御方法を提供することにある。

【課題を解決するための手段】

【0009】

上記の課題を解決するために、請求項1に記載の発明では、通信機能を有する携帯機との通信により、携帯機に設定されたIDコードと自身の記録手段に既に記録されているIDコードとの照合を行い、該照合の成立の有無に基づいてセキュリティ機器を制御するセキュリティ制御装置と、該セキュリティ制御装置との通信を行うことにより、対応する前記携帯機の管理を行う携帯機管理装置とを備えたセキュリティ制御システムであって、前記セキュリティ制御装置は、前記携帯機に設定されたIDコードを前記記録手段に記録するID登録制御を行い、該ID登録制御時にあっては、登録対象となるIDコードを含む登録信号を前記携帯機管理装置に送信し、該携帯機管理装置は、前記登録信号に基づいて、対応する携帯機の管理を行うことを要旨とする。

10

【0010】

請求項2に記載の発明では、請求項1に記載のセキュリティ制御システムにおいて、前記セキュリティ制御装置は、前記ID登録制御時にあっては、登録を完了したIDコードを含む前記登録信号を前記携帯機管理装置に送信し、前記携帯機管理装置は、前記登録信号を受信した際に、該登録信号に含まれるIDコードの登録が妥当か否かの判断を行い、該登録が妥当ではないと判断した際に、異常登録がなされた旨を示す異常報知信号を、ユーザが所持する携帯通信機器に通報する通報制御を行うことを要旨とする。

20

【0011】

請求項3に記載の発明では、請求項1に記載のセキュリティ制御システムにおいて、前記セキュリティ制御装置は、前記ID登録制御時にあっては、登録許可要求信号を前記携帯機管理装置に送信し、前記携帯機管理装置は、前記登録許可要求信号を受信した際に、前記IDコードの登録が妥当か否かの判断を行うとともに、その判断結果を示す応答信号を前記セキュリティ制御装置に送信し、前記セキュリティ制御装置は、前記IDコードの登録が妥当である旨を含む前記応答信号を受信したことを条件として、該IDコードを前記記録手段に記録することを要旨とする。

【0012】

請求項4に記載の発明では、請求項1～3のいずれか1項に記載のセキュリティ制御システムにおいて、前記携帯機管理装置は、ユーザが所持する携帯通信機器から送信される制限要求信号を受信する受信手段を備え、該受信手段により該制限要求信号を受信したことを条件として前記セキュリティ制御装置に機能制限信号を送信し、前記セキュリティ制御装置は、前記機能制限信号を受信したことを条件として、前記セキュリティ機器によるセキュリティ解除動作を禁止または制限することを要旨とする。

30

【0013】

請求項5に記載の発明では、固有のIDコードが設定された携帯機との通信を行う携帯機用通信手段と、前記IDコードと対応するIDコードが記録される記録手段と、前記携帯機との通信時に、携帯機に設定されたIDコードと前記記録手段に記録されたIDコードとの照合を行い、該照合が一致したか否かに基づいてセキュリティ機器を制御するセキュリティ制御手段とを備えるセキュリティ制御装置であって、当該セキュリティ制御装置の外部に配設されるとともに、前記記録手段に記録されたIDコードに基づいて前記携帯機の管理を行う携帯機管理装置と通信可能なセキュリティ通信手段と、前記携帯機のIDコードを前記記録手段に記録するID登録制御を行うとともに、そのID登録制御の際に、該記録対象となるIDコードを含む登録信号を、前記セキュリティ通信手段を介して前記携帯機管理装置に送信する登録通信制御を行う登録制御手段とを備えることを要旨とする。

40

【0014】

請求項6に記載の発明では、請求項5に記載のセキュリティ制御装置において、前記登

50

録制御手段は、前記ID登録制御時に、前記セキュリティ通信手段から前記携帯機管理装置に登録許可要求信号を送信する一方、該登録許可要求信号に応答して送信された前記携帯機管理装置からの応答信号が前記セキュリティ通信手段によって受信され、その応答信号に登録許可の旨が含まれていることを条件として、前記IDコードを前記記録手段に登録することを要旨とする。

【0015】

請求項7に記載の発明では、請求項5または請求項6に記載のセキュリティ制御装置において、前記セキュリティ制御手段は、前記携帯機管理装置から送信される機能制限信号が前記セキュリティ通信手段によって受信されたことを条件として、前記セキュリティ機器によるセキュリティ解除動作を禁止または制限することを特徴とする。 10

【0016】

請求項8に記載の発明では、通信機能を有する携帯機との通信に基づき、該携帯機に設定されたIDコードと自身に予め登録されたIDコードとの照合結果に基づいてセキュリティ機器を制御するとともに、前記IDコードの登録時に該IDコードを含む登録信号を外部に送信するセキュリティ制御装置と通信可能な管理通信手段と、前記登録信号を前記管理通信手段により受信した際に、該登録信号に含まれるIDコードに基づいて該携帯機の管理を行う管理手段とを備えることを要旨とする。

【0017】

請求項9に記載の発明では、請求項8に記載の携帯機管理装置において、ユーザによって所持される携帯通信機器との通信を行う携帯機器用通信手段を備え、前記管理手段は、前記管理通信手段によって前記登録信号を受信した際に該登録信号に含まれるIDコードの登録が妥当か否かの判断を行い、該登録が妥当ではないと判断した際に、異常登録がなされた旨を示す異常報知信号を、前記携帯機器用通信手段から前記携帯機器に送信させる異常報知制御を行うことを要旨とする。 20

【0018】

請求項10に記載の発明では、請求項8に記載の携帯機管理装置において、前記管理手段は、前記携帯機のIDコードの登録時に前記セキュリティ制御装置から送信される登録許可要求信号を前記管理通信手段によって受信した際に、前記IDコードの登録が妥当か否かの判断を行うとともに、その判断結果を示す応答信号を前記セキュリティ制御装置に送信することを要旨とする。 30

【0019】

請求項11に記載の発明では、請求項8～請求項10に記載の携帯機管理装置において、ユーザが所持する携帯通信機器から送信される制限要求信号を受信する受信手段を備え、前記管理手段は、前記受信手段により前記制限要求信号を受信したことを条件として、前記セキュリティ機器によるセキュリティ解除動作を禁止または制限させるための機能制限信号を、前記セキュリティ制御装置及び前記携帯機のうちの少なくとも一方に送信することを要旨とする。

【0020】

請求項12に記載の発明では、通信機能を有する携帯機との通信により、携帯機に設定されたIDコードと自身の記録手段に既に記録されているIDコードとの照合を行い、該照合の成立の有無に基づいてセキュリティ機器を制御するセキュリティ制御装置と、該セキュリティ制御装置との通信を行うことにより前記携帯機の管理を行う携帯機管理装置とを備えたセキュリティ制御システムにおけるセキュリティ制御方法であって、前記携帯機に設定されたIDコードを前記記録手段に登録するID登録制御を前記セキュリティ制御装置により行い、該ID登録制御時に、登録対象となるIDコードを含む登録信号を該セキュリティ制御装置から前記携帯機管理装置に送信し、前記登録信号に含まれるIDコードと対応する携帯機の管理を、前記携帯機管理装置によって行うことを要旨とする。 40

【0021】

以下、本発明の「作用」について説明する。

請求項 1 または請求項 1 2 に記載の発明によると、セキュリティ制御装置は、携帯機との通信が成立したか否かに基づいて、セキュリティ機器を制御する。そして、携帯機とセキュリティ制御装置との通信を成立させるためには、携帯機の ID コードをセキュリティ制御装置の記録手段に記録する ID 登録が必要となる。この ID 登録時には、登録対象となる ID コードを含む登録信号がセキュリティ制御装置から携帯機管理装置に送信される。そして、携帯機管理装置は、該登録信号に基づいて、対応する携帯機の管理を行う。このため、携帯機の ID コードがセキュリティ制御装置に不正に登録された場合、携帯機管理装置によって該不正登録を認識可能となる。よって、例えば、ID コードの不正登録が行われた際に、その旨を携帯機管理装置から通知させたり、該不正登録された携帯機との通信に基づいてセキュリティ制御装置がセキュリティ機器を制御できないようにする制限制御を携帯機管理装置によって行わせたりすることが可能となる。それゆえ、セキュリティ機器のセキュリティレベルをより一層向上させることが可能となる。

10

#### 【0022】

請求項 2 に記載の発明によると、携帯機の ID コードがセキュリティ制御装置に不正に登録されると、異常登録がなされた旨を示す異常報知信号が、携帯機管理装置からユーザが所持する携帯通信機器に通報される。このため、ユーザは、携帯機の ID コードが不正に登録された旨を、携帯通信機器を通じて確実且つ迅速に認識することができる。よって、該不正登録に対する迅速な対応が可能となり、セキュリティ機器のセキュリティレベルをより一層向上させることが可能となる。

20

#### 【0023】

請求項 3 に記載の発明によると、ID 登録制御時にあっては、登録対象となる ID コードの登録が妥当か否かの判断が携帯機管理装置によって行われ、該 ID コードの登録が妥当であると判断されないと、セキュリティ制御装置は、該 ID コードを記録手段に記録することができない。このため、ID コードの不正な登録が抑止され、セキュリティ機器のセキュリティレベルが向上する。

#### 【0024】

請求項 4 に記載の発明によると、ユーザが所持する携帯通信機器から送信される制限要求信号が携帯機管理装置によって受信されると、携帯機管理装置からセキュリティ制御装置に対して機能制限信号が送信される。セキュリティ制御装置は、機能制限信号を受信したことを条件として、セキュリティ機器によるセキュリティ解除動作を禁止または制限する。このため、ユーザが携帯機を紛失したり盗難されたりした場合には、携帯通信機器から制限要求信号を送信させることにより、セキュリティ解除動作を禁止または制限することができる。よって、携帯機の紛失・盗難時においても、該携帯機によるセキュリティ解除動作を即座に禁止または制限することができ、セキュリティ機器の高いセキュリティレベルを確保することができる。

30

#### 【0025】

請求項 5 に記載の発明によると、セキュリティ制御装置は、携帯機との通信が成立したか否かに基づいて、セキュリティ機器を制御する。そして、携帯機とセキュリティ制御装置との通信を成立させるためには、携帯機の ID コードをセキュリティ制御装置の記録手段に記録する ID 登録が必要となる。この ID 登録時には、登録対象となる ID コードを含む登録信号がセキュリティ制御装置から携帯機管理装置に送信される。これにより、携帯機管理装置は、該登録信号に基づいて、対応する携帯機の管理を行うことが可能となる。このため、携帯機の ID コードがセキュリティ制御装置に不正に登録された場合、携帯機管理装置によって該不正登録を認識可能となる。よって、例えば、ID コードの不正登録が行われた際に、その旨を携帯機管理装置から通知させたり、該不正登録された携帯機との通信に基づいてセキュリティ制御装置がセキュリティ機器を制御できないようにする制限制御を携帯機管理装置によって行わせたりすることが可能となる。それゆえ、セキュリティ機器のセキュリティレベルをより一層向上させることが可能となる。

40

#### 【0026】

請求項 6 に記載の発明によると、ID 登録制御時にあっては、セキュリティ通信手段か

50



ら携帯機管理装置に登録許可要求信号が送信される。そして、登録制御手段は、携帯機管理装置から送信される登録許可の旨を含む応答信号をセキュリティ通信手段によって受信しないと、登録対象となる携帯機のIDコードを記録手段に記録しない。すなわち、登録制御手段が携帯機のIDコードを記録手段に記録するためには、携帯機管理装置による許可が必要となり、携帯機とセキュリティ制御装置との通信のみによってはIDコードの登録を行うことができない。よって、IDコードの不正な登録が抑止され、セキュリティ機器のセキュリティレベルがより一層向上する。

#### 【0027】

請求項7に記載の発明によると、携帯機管理装置からセキュリティ制御装置に対して機能制限信号が送信されると、セキュリティ制御装置は、セキュリティ機器によるセキュリティ解除動作を禁止または制限する。このため、ユーザが携帯機を紛失したり盗難されたりした場合、携帯機管理装置からセキュリティ制御装置に機能制限信号を送信させることにより、セキュリティ解除動作を禁止または制限することができる。よって、携帯機の紛失・盗難時においても、該携帯機によるセキュリティ解除動作を即座に禁止または制限することができ、セキュリティ機器の高いセキュリティレベルを確保することができる。

10

#### 【0028】

請求項8に記載の発明によると、セキュリティ制御装置から送信される登録信号が管理通信手段によって受信される。そして、その登録信号に含まれる携帯機固有のIDコードに基づく該携帯機の管理が、管理手段によって行われる。それゆえ、管理手段は、セキュリティ制御装置に登録されたIDコードを認識可能となり、携帯機のIDコードがセキュリティ制御装置に不正に登録された場合には、その旨を認識可能となる。よって、例えば、IDコードの不正登録が行われた際に、その旨を携帯機管理装置から通知させたり、該不正登録された携帯機との通信に基づいてセキュリティ制御装置がセキュリティ機器を制御できないようにする制限制御を携帯機管理装置によって行わせたりすることが可能となる。それゆえ、セキュリティ機器のセキュリティレベルをより一層向上させることが可能となる。

20

#### 【0029】

請求項9に記載の発明によると、管理手段は、セキュリティ制御装置に対する携帯機のIDコードの登録が妥当ではないと判断した場合、セキュリティ制御装置にIDコードが不正に登録されたと判断する。そしてこの場合、異常登録がなされた旨を示す異常報知信号が、携帯機管理装置からユーザが所持する携帯通信機器に送信される。このため、ユーザは、携帯機のIDコードが不正に登録された旨を、携帯通信機器を通じて確実且つ迅速に認識することができる。よって、該不正登録に対する迅速な対応が可能となり、セキュリティ機器のセキュリティレベルをより一層向上させることが可能となる。

30

#### 【0030】

請求項10に記載の発明によると、携帯機のIDコードのセキュリティ制御装置への登録時にあっては、登録対象となるIDコードの登録が妥当か否かの判断が管理手段によって行われ、その判断結果を示す応答信号がセキュリティ制御装置に送信される。このため、例えば、IDコードの登録が妥当である旨の判断結果を示す応答信号を受信しない限りIDコードの登録を行えないようにセキュリティ制御装置が構成されていれば、管理手段によってIDコードの登録が妥当であると判断されないと、該IDコードの登録を行うことができない。よって、IDコードの不正な登録が抑止され、セキュリティ機器のセキュリティレベルがより一層向上する。

40

#### 【0031】

請求項11に記載の発明によると、例えば機能制限信号を受信したことを条件として、セキュリティ機器によるセキュリティ解除動作を禁止または制限するようにセキュリティ制御装置を構成すれば、ユーザは、携帯通信機器から制限要求信号を送信させれば、該セキュリティ解除動作を容易に禁止または制限させることが可能となる。また、例えば機能制限信号を受信したことを条件として、セキュリティ制御装置との通信を禁止するように携帯機を構成すれば、ユーザは、携帯通信機器から制限信号を送信させれば、該セキュリ

50

ティ解除動作を容易に禁止または制限させることが可能となる。

【発明の効果】

【0032】

以上詳述したように、本発明によれば、セキュリティ機器のセキュリティレベルをより一層向上させることができる。

【発明を実施するための最良の形態】

【0033】

（第1実施形態）

以下、本発明を車両用セキュリティ制御システムに具体化した第1実施形態を、図1及び図2に基づき詳細に説明する。

【0034】

図1に示すように、車両用セキュリティ制御システム1は、車両2のユーザ（オーナー）によって所持される携帯機3と、車両2に設けられたセキュリティ制御装置10と、車両外部の所定箇所に設けられた携帯機管理装置30とを備えている。

【0035】

携帯機3は通信機能を有し、セキュリティ制御装置10から送信されるリクエスト信号を受信可能となっている。そして、携帯機3は、該リクエスト信号を受信すると、自身に予め設定されたIDコードを含むIDコード信号を送信する。また、携帯機3は、自身に設けられた操作部が操作されると、IDコードと、施錠コードまたは解錠コードとを含む施解錠指令信号を送信する。

【0036】

セキュリティ制御装置10は、携帯機用通信手段としての送信回路11及び受信回路12と、セキュリティ制御手段及び登録制御手段としての車両制御部13と、セキュリティ通信手段としてのセキュリティ通信部14とを備えている。そして、車両制御部13には、送信回路11、受信回路12及びセキュリティ通信部14が電氣的に接続されている。

【0037】

送信回路11は、車両制御部13から出力されるリクエスト信号を所定周波数（ここでは134kHz）の電波に変換し、送信アンテナ11aを介して、車両2の周辺の所定領域及び車両2の室内に選択的に該電波を送信する。

【0038】

受信回路12は、携帯機3から送信されるIDコード信号及び施解錠指令信号を、受信アンテナ12aを介して受信し、その受信信号をパルス信号に復調して車両制御部13へ出力する。

【0039】

セキュリティ通信部14は、携帯機管理装置30と通信可能に構成されている。そして、セキュリティ通信部14は、車両制御部13から登録信号が入力されると、その登録信号を所定周波数の電波に変調し、該電波を携帯機管理装置30に送信する。また、セキュリティ通信部14は、携帯機管理装置30から送信される送信信号を受信すると、該送信信号をパルス信号に復調し、該復調した信号を車両制御部13に出力する。

【0040】

車両制御部13は、具体的には図示しないCPU、ROM、RAMからなるCPUユニットであり、記録手段としての不揮発性のメモリ13aを備えている。このメモリ13aには、携帯機3に設定されたIDコードを1つまたは複数個記録可能となっている。

【0041】

また、車両制御部13には、モードスイッチ21と、セキュリティ機器としてのドアロック駆動装置22及びエンジン制御部23とが電氣的に接続されている。

モードスイッチ21はユーザによって操作可能なスイッチであり、本実施形態においては車両2の室内に設けられている。そして、このモードスイッチ21が操作されると、該モードスイッチ21から車両制御部13に対して操作信号が出力される。

【0042】

10

20

30

40

50

ドアロック駆動装置 22 は、図示しないアクチュエータに接続され、車両制御部 13 から駆動信号が入力されると、該アクチュエータを駆動してドア錠を自動的に施解錠する。また、ドアロック駆動装置 22 は、ドア錠の施解錠状態を示す施解錠状態信号を車両制御部 13 に出力する。このため、車両制御部 13 は、該施解錠状態信号に基づき、ドア錠の施解錠状態を認識可能となる。

【0043】

エンジン制御部 23 は、図示しないセルモータに接続され、車両制御部 13 から始動信号が入力されると、同セルモータを駆動するとともに、燃料噴射制御や点火制御を行って、エンジンを自動的に始動させる。また、エンジン制御部 23 は、エンジンの駆動状態を示す駆動状態信号を車両制御部 13 に出力する。このため、車両制御部 13 は、該駆動状態信号に基づき、エンジンの駆動状態を認識可能となる。

10

【0044】

車両制御部 13 は、ドアロック駆動装置 22 やエンジン制御部 23 を制御するセキュリティ制御モードと、携帯機 3 に設定された ID コードをメモリ 13a に記録（登録）する ID 登録制御を行う ID 登録モードとを有している。そして、車両制御部 13 は、モードスイッチ 21 から操作信号が入力された際に ID 登録モードとなり、それ以外はセキュリティ制御モードとなる。

【0045】

セキュリティ制御モードにおいて車両制御部 13 は、送信回路 11 に対してリクエスト信号を間欠的に出力する。このため、送信回路 11 及び送信アンテナ 11a を介して、車両 2 の周辺の所定領域及び車両 2 の室内に選択的にリクエスト信号が送信される。また、車両制御部 13 は、受信回路 12 から前記 ID コード信号または施解錠指令信号が入力されると、それらの信号に含まれる ID コードと、メモリ 13a に記録されている ID コードとの比較（ID コード照合）を行う。そして、車両制御部 13 は、それら ID コード同士が一致したこと、すなわち ID コードの照合が成立したことを条件として、ドアロック駆動装置 22 やエンジン制御部 23 の駆動制御を行う。

20

【0046】

詳しくは、ID コード信号が入力された場合、車両制御部 13 は、該 ID コード信号が、車両 2 の周辺の所定領域に送信されたリクエスト信号に応答したものであれば、ドアロック駆動装置 22 に駆動信号を出力してドア錠を解錠させる。そして、車両制御部 13 は、該 ID コード信号が入力されなくなると、ドアロック駆動装置 22 に駆動信号を出力してドア錠を施錠させる。

30

【0047】

これに対し、車両制御部 13 は、入力された ID コード信号が、車両 2 の室内に送信されたリクエスト信号に応答したものであれば、エンジン始動待機状態となる。そして、車両制御部 13 は、このエンジン始動待機状態において図示しないスタートスイッチから操作信号が入力されると、エンジン制御部 23 に対して始動信号を出力してエンジンを始動させる。つまり、車両制御部 13 は、エンジン始動待機状態でない場合には、たとえスタートスイッチから操作信号が入力されてもエンジン制御部 23 に始動信号を出力しない。なお、スタートスイッチは、車両 2 の室内において運転席の近辺に設けられたスイッチであり、車両制御部 13 と電氣的に接続されている。

40

【0048】

また、施解錠指令信号が入力された場合、車両制御部 13 は、該施解錠指令信号に施錠コードが含まれていればドア錠を施錠させ、解錠コードが含まれていればドア錠を解錠させる。

【0049】

このように、セキュリティ制御モードにおいてセキュリティ制御装置 10 は、携帯機 3 との通信を行い、該携帯機 3 との通信の成立有無に基づいてドアロック駆動装置 22 やエンジン制御部 23 といったセキュリティ機器を制御する。

【0050】

50

一方、セキュリティ制御モードからID登録モードに切り換わると、車両制御部13は、送信回路11に対してリクエスト信号を間欠的に出力し、セキュリティ制御モードと同様に携帯機3との通信を行う。そして、車両制御部13は、受信回路12からIDコード信号が入力されると、該IDコード信号に含まれるIDコードをメモリ13aに記録する。該記録を完了すると、車両制御部13は、セキュリティ通信部14に対して該IDコードと車両情報とを含む登録信号を出力し、該セキュリティ通信部14を介して登録信号を携帯機管理装置30に送信する登録通信制御を行う。なお、車両情報とは車両2を特定するための情報であり、本実施形態において車両情報には、車両2の車体番号、車両番号、ディーラー情報（ディーラーに固有に設定された店舗番号やパスワード等）のうちの少なくとも1つが含まれている。

10

#### 【0051】

携帯機管理装置30は専用の管理センターなどに配設されており、管理通信手段としての管理通信部31と、管理手段としての管理制御部32と、携帯機器用通信手段としての携帯機器用通信部33とを備えている。そして、管理制御部32には、管理通信部31及び携帯機器用通信部33が電氣的に接続されている。

#### 【0052】

管理通信部31は、セキュリティ制御装置10のセキュリティ通信部14と通信可能となっており、該セキュリティ通信部14から送信される登録信号を受信すると、その登録信号を復調して管理制御部32に出力する。

#### 【0053】

携帯機器用通信部33は、ユーザによって所持される携帯通信機器（ここでは携帯電話4）と通信可能となっている。そして、携帯機器用通信部33は、管理制御部32から異常報知信号が入力されると、その異常報知信号を、公衆通信回線などを用いて携帯電話4に送信する。

20

#### 【0054】

管理制御部32は、具体的には図示しないCPU、ROM、RAMからなるCPUユニットであり、不揮発性のメモリ32aを備えている。

このメモリ32aには、管理対象として設定された車両2の車両情報、該車両情報に対応して設定された登録認否情報、及び該車両2に搭載されたセキュリティ制御装置10のメモリ13aに記録されたIDコードが記録されている。詳しくは、メモリ32aには、車両情報として、車両2の車体番号、車両番号、ディーラー情報（ディーラーに固有に設定された店舗番号やパスワード等）、前記携帯電話4の機器情報（電話番号、メールアドレス等）など、車両2を特定するための情報が記録されている。

30

#### 【0055】

登録認否情報は、IDコードの登録を認可するか不認可とするかを示す情報であり、携帯電話4から送信される。この登録認否情報は、ユーザによって設定可能となっている。具体的には、登録認否情報は、所定桁数の暗証コードからなり、携帯電話4のテンキーから入力される暗証番号をバイナリー変換したものに相当する。また、該登録認否情報は、IDコードの登録を認可する登録認可コードと、IDコードの登録を不認可とする登録不認可コードとの2種類が存在し、それぞれユーザによって設定可能な暗証番号と対応している。このため、ユーザは、登録認可コードとしての暗証番号と、登録不認可コードとしての暗証番号を自由に設定することができる。なお、本実施形態において携帯電話4は、所定の認否情報送信操作（例えば、携帯機管理装置30への電話番号入力や、所定のコマンド入力など）が行われた際に、登録認否情報を携帯機管理装置30に送信するようになっている。

40

#### 【0056】

メモリ32aには、該車両情報に対応して、IDコードの記録領域及び登録認否情報の記録領域が設定されている。例えば、メモリ32aに2台の車両2の車両情報A、Bが記録されている場合、車両情報Aに対応するIDコードの記録領域及び登録認否情報の記録領域と、車両情報Bに対応するIDコードの記録領域及び登録認否情報の記録領域とが個

50

別に設定されている。なお、該IDコードの記録領域には、複数のIDコードを記録可能となっており、その記録可能なIDコードの数は、予め設定された規定数またはユーザによって設定された規定数となっている。また、該記録領域に記録されるIDコードには、例えば記録された順番などからなる登録番号が対応付けされている。

【0057】

管理制御部32は、携帯電話4から送信される登録認否情報が携帯機器用通信部33を介して入力されると、その登録認否情報をメモリ32aに記録する。なお、管理制御部32は、登録認否情報が入力される度に、最新の登録認否情報をメモリ32aに更新記録（上書き保存）する。

【0058】

また、管理制御部32は、管理通信部31から登録信号が入力されると、該登録信号に含まれる車両情報に基づき、対応する登録認否情報が登録認可コードであり、且つ対応するIDコードの記録領域に空き領域が存在する場合には、同登録信号に含まれるIDコードを該空き領域に記録する。すなわち、こうした場合、管理制御部32は、IDコードの登録が妥当であると判断する。そして、管理制御部32は、該記録が完了した旨を示す登録完了信号を、管理通信部31を介してセキュリティ制御装置10に送信する。一方、管理制御部32は、車両情報と対応するIDコードの記録領域に空き領域がない場合や、対応する登録認否情報が登録不認可コードである場合には、IDコードの異常登録が行われたと判断する。すなわち、こうした場合、管理制御部32は、IDコードの登録が妥当ではないと判断する。そして、管理制御部32は、該異常登録が行われた旨を示す異常報知信号を携帯機器用通信部33に出力する。よって、携帯機器用通信部33から携帯電話4に異常報知信号が送信される。

【0059】

次に、このように構成された車両用セキュリティ制御システム1において、携帯機3のIDコードをセキュリティ制御装置10に登録する際に行われる通信態様を、図2に示すシーケンスチャートを用いて説明する。

【0060】

まず、セキュリティ制御装置10のモードスイッチ21がユーザによって操作されると（ステップS1）、セキュリティ制御装置10はセキュリティ制御モードからID登録モードに切り換わる（ステップS2）。ID登録モードに切り換わるとセキュリティ制御装置10は、車両2の室内に前記リクエスト信号を送信する（ステップS3）。

【0061】

そして、携帯機3は、このリクエスト信号を受信すると、前記IDコード信号を送信する（ステップS4）。

セキュリティ制御装置10は、携帯機3からのIDコード信号を受信すると、該IDコード信号に含まれるIDコードをメモリ13aに記録する（ステップS5）。すなわち、セキュリティ制御装置10は、取得した携帯機3のIDコードを自身に登録する。次いで、セキュリティ制御装置10は、携帯機管理装置30に前記登録信号を送信する（ステップS6）。

【0062】

携帯機管理装置30は、セキュリティ制御装置10からの登録信号を受信すると、該登録信号に含まれる車両情報に基づき、対応するセキュリティ制御装置10へのIDコードの登録が認可状態であるか否かを判断する（ステップS7）。すなわち、ここで携帯機管理装置30は、車両情報に対応する登録認否情報が登録認可コードであるか否かを判断する。また、携帯機管理装置30は、メモリ32aにおけるIDコードの記録領域を割り出し、登録信号に含まれるIDコードを該記録領域に記録可能であるか否かを判断する（同ステップS7）。すなわち、ここで携帯機管理装置30は、該記録領域にIDコードを登録可能な領域が存在するか否かを判断する。その結果、対応する登録認否情報が登録認可コードであり、且つメモリ32aにおいて車両情報と対応するIDコードの記憶領域に空き領域が存在する場合、携帯機管理装置30は、IDコードの登録が妥当であると判断し

10

20

30

40

50

、取得したIDコードを該空き領域に記録する（ステップS8）。また、携帯機管理装置30は、前記登録完了信号をセキュリティ制御装置10に送信する（ステップS9）。このため、携帯機管理装置30は、記録したIDコードに基づき、車両2に対応する携帯機3の管理が可能となる。

#### 【0063】

セキュリティ制御装置10は、携帯機管理装置30からの登録完了信号を受信すると、車両2の室内に設けられた図示しないインジケータに登録完了の旨を示す表示を行ったり、図示しないスピーカなどから該登録完了の旨を示す音響報知を行ったりする（ステップS10）。このため、ユーザは、携帯機3の登録が完了したことを確実に認識可能となる。

10

#### 【0064】

一方、携帯機管理装置30は、ステップS7において車両情報に対応する登録認否情報が登録不認可コードである場合や、対応するIDコードの記録領域にIDコードを登録可能な領域が存在しない場合には、IDコードの登録が妥当ではないと判断し、前記異常報知信号を携帯電話4に送信する（ステップS11）。このため、携帯電話4には、IDコードの異常登録があった旨が示される。よって、例えば第三者によって不正にIDコードの登録が行われた場合、ユーザは、たとえ車両から離間していても、該不正登録の旨を迅速且つ確実に認識することができる。

#### 【0065】

したがって、本実施形態によれば以下の効果を得ることができる。

20

(1) セキュリティ制御装置10は、携帯機3との通信が成立したか否かに基づいて、ドアロック駆動装置22やエンジン制御部23といったセキュリティ機器を制御する。そして、携帯機3とセキュリティ制御装置10との通信を成立させるためには、携帯機3のIDコードをセキュリティ制御装置10の車両制御部13のメモリ13aに記録するID登録が必要となる。このID登録時には、登録対象となるIDコードを含む登録信号がセキュリティ制御装置10から携帯機管理装置30に送信される。そして、携帯機管理装置30は、該登録信号を受信すると、該登録信号に含まれるIDコードを管理制御部32のメモリ32aに記録し、該記録したIDコードに基づいて対応する携帯機3の管理を行う。このため、携帯機3のIDコードがセキュリティ制御装置10に不正に登録された場合、携帯機管理装置30によって該不正登録を認識することができる。よって、第三者によるIDコードの不正登録を抑止することができ、セキュリティ機器のセキュリティレベルをより一層向上させることができる。

30

#### 【0066】

(2) 携帯機管理装置30における管理制御部32のメモリ32aに、登録不認可コードからなる登録認否情報が記録されている場合、携帯機管理装置30は、セキュリティ制御装置10へのIDコードの登録を不認可とする登録不認可状態となる。しかし、この登録不認可状態にも拘わらず、セキュリティ制御装置10から登録信号が入力されると、携帯機管理装置30は、IDコードの不正登録が行われたと判断し、その旨を携帯電話4に通知する。すなわち、IDコードの不正登録が行われた場合、その旨が携帯電話4に通報される。このため、ユーザは、たとえ車両2から離間していても、IDコードの不正登録が行われたことを携帯電話4を通じて迅速且つ確実に認識することができ、該不正登録に対する迅速な対応が可能となる。よって、セキュリティ機器のセキュリティレベルをより一層向上させることができる。

40

#### 【0067】

(3) 携帯電話4に暗証番号が入力されると、該携帯電話4から携帯機管理装置30に対して登録認否情報が送信される。そして、携帯機管理装置30は、該登録認否情報に基づいて、IDコードの登録認可状態と、IDコードの登録不認可状態とのうちのいずれかに切り換わるようになっている。つまり、携帯機管理装置30におけるIDコードの登録認可状態、登録不認可状態を、ユーザによって設定可能となっている。このため、例えばユーザは、IDコードの登録が必要な場合にのみ携帯機管理装置30を登録認可状態にす

50

ることができる。よって、セキュリティ機器のセキュリティレベルをさらに向上させることができる。

【0068】

(4) セキュリティ制御装置10及び携帯機管理装置30へのIDコードの登録完了時には、車両2の室内に設けられたインジケータにその旨が表示される。このため、ユーザは、該インジケータを視認することにより、IDコードの登録が完了した旨を確実に認識することができる。

【0069】

(第2実施形態)

次に、本発明を具体化した第2実施形態を図1及び図3に基づいて説明する。なお、以下の各実施形態では、第1実施形態と相違する点を主に述べ、共通する点については同一部材番号を付すのみとしてその説明を省略する。

【0070】

本実施形態において前記第1実施形態と異なる点は、セキュリティ制御装置10の車両制御部13及び携帯機管理装置30の管理制御部32によって行われる制御態様と、携帯機3のIDコードをセキュリティ制御装置10に登録する制御(ID登録制御)時に行われる車両用セキュリティ制御システム1の通信態様とについてである。なお、携帯機3、セキュリティ制御装置10及び携帯機管理装置30のハードウェア構成については第1実施形態と同じである。

【0071】

そこで、まず車両制御部13及び管理制御部32によって行われる制御について説明する。

車両制御部13は、セキュリティ制御モードにおいては前記第1実施形態と同様の制御を行う。これに対し、モードスイッチ21が操作されてセキュリティ制御モードからID登録モードに切り換わると、車両制御部13は、車両情報を含む登録許可要求信号をセキュリティ通信部14に出力する。このため、セキュリティ通信部14から携帯機管理装置30に該登録許可要求信号が送信される(図1参照)。

【0072】

また、車両制御部13は、登録許可要求信号を出力した後、セキュリティ通信部14から応答信号が入力されると、該応答信号に許可コードが含まれているか否かを判断する。そして、車両制御部13は、該応答信号に許可コードが含まれていると判断すると、送信回路11に対してリクエスト信号を間欠的に出力し、前記第1実施形態と同様に携帯機3との通信を行う。そして、車両制御部13は、携帯機3から送信されたIDコード信号が受信回路12から入力されると、該IDコード信号に含まれるIDコードをメモリ13aに記録する。該記録が完了すると、車両制御部13は、セキュリティ通信部14に対して該IDコードと車両情報とを含む登録信号を出力し、該セキュリティ通信部14を介して該登録信号を携帯機管理装置30に送信する。

【0073】

これに対し、車両制御部13は、該許可コードを含む応答信号を受信できない場合には、ID登録モードにおける携帯機3との通信を禁止するとともに、車両2の室内に設けられた図示しないインジケータに、IDコードの登録が禁止状態である旨を示す表示を行う。このため、携帯機管理装置30によってIDコードの登録が禁止されている状態にあつては、車両制御部13のメモリ13aには新たなIDコードの記録されない。また、ユーザは、インジケータを視認することにより、該記録が禁止されている旨を確実に認識可能となる。

【0074】

一方、管理制御部32は、セキュリティ制御装置10からの登録許可要求信号が入力されると、メモリ32aに記録されている登録認否情報のうち、該登録許可要求信号に含まれる車両情報と対応する登録認否情報が登録認可コードであり、且つ対応するIDコードの記録領域に空き領域が存在するか否かの判断(認証)を行う。そして、該認証が成立す



ると、管理制御部 3 2 は、許可コードを含む応答信号を、管理通信部 3 1 を介してセキュリティ制御装置 1 0 に送信する（図 1 参照）。これに対し、該認証が成立しない場合、すなわち車両情報と対応する ID コードの記録領域に空き領域がない場合や、対応する登録認否情報が登録不認可コードである場合、管理制御部 3 2 は、応答信号を送信しない。さらにこの場合、管理制御部 3 2 は、ID コードの異常登録が行われようとしていると判断し、その旨を示す異常報知信号を携帯機器用通信部 3 3 に出力する。よって、携帯機器用通信部 3 3 から携帯電話 4 に異常報知信号が送信される。

【0075】

また、管理制御部 3 2 は、管理通信部 3 1 を介してセキュリティ制御装置 1 0 から登録信号が入力されると、同登録信号に含まれる ID コードを該空き領域に記録する。そして、管理制御部 3 2 は、該記録が完了した旨を示す登録完了信号を、管理通信部 3 1 を介してセキュリティ制御装置 1 0 に送信する。

【0076】

次に、本実施形態の車両用セキュリティ制御システム 1 の ID 登録制御時における通信様を、図 3 に示すシーケンスチャートを用いて説明する。

まず、セキュリティ制御装置 1 0 のモードスイッチ 2 1 がユーザによって操作されると（ステップ S 2 1）、セキュリティ制御装置 1 0 はセキュリティ制御モードから ID 登録モードに切り換わる（ステップ S 2 2）。ID 登録モードに切り換わるとセキュリティ制御装置 1 0 は、登録許可要求信号を携帯機管理装置 3 0 に送信する（ステップ S 2 3）。

【0077】

携帯機管理装置 3 0 は、該登録許可要求信号を受信すると、該登録許可要求信号に含まれる車両情報に基づき、対応するセキュリティ制御装置 1 0 への ID コードの登録が認可状態であるか否かの判断（認証）を行う（ステップ S 2 4）。すなわち、ここで携帯機管理装置 3 0 は、車両情報に対応する登録認否情報が登録認可コードであるか否かを判断する。また、携帯機管理装置 3 0 は、メモリ 3 2 a における ID コードの記録領域を割り出し、該記録領域に新たに ID コードを記録可能であるか否かを判断する（同ステップ S 2 4）。すなわち、ここで携帯機管理装置 3 0 は、該記録領域に新規の ID コードを登録可能な領域が存在するか否かを判断する。その結果、対応する登録認否情報が登録認可コードであり、且つメモリ 3 2 a において車両情報と対応する ID コードの記憶領域に空き領域が存在する場合、携帯機管理装置 3 0 は、ID コードの登録が妥当である（認証 OK）と判断し、許可コードを含む応答信号をセキュリティ制御装置 1 0 に送信する（ステップ S 2 5）。

【0078】

これに対し、携帯機管理装置 3 0 は、車両情報に対応する登録認否情報が登録不認可コードである場合や、対応する ID コードの記録領域に ID コードを登録可能な領域が存在しない場合には、ID コードの登録が妥当ではない（認証 NG）と判断し、許可コードを含む応答信号をセキュリティ制御装置 1 0 に送信しない。また、この場合、携帯機管理装置 3 0 は、異常報知信号を携帯電話 4 に送信する（ステップ S 2 6）。このため、携帯電話 4 には、ID コードの異常登録が行われようとしている旨が示される。よって、例えばセキュリティ制御装置 1 0 が第三者によって不正に ID 登録モードに切り換えられた場合など、ユーザの意に反して ID 登録モードに切り換わった場合には、ユーザは、たとえ車両から離間していても、該 ID 登録モードへの遷移の旨を、迅速且つ確実に認識することができる。すなわち、本実施形態では、携帯機 3 の ID コードがセキュリティ制御装置 1 0 に登録される以前に、ユーザに対して異常報知がなされる。このため、ID コードの不正な登録を未然に防ぐことが可能となる。

【0079】

ところで、携帯機管理装置 3 0 から許可コードを含む応答信号が送信された場合、セキュリティ制御装置 1 0 によって該応答信号が受信されると、セキュリティ制御装置 1 0 は、車両 2 の室内に前記リクエスト信号を送信する（ステップ S 2 7）。

【0080】

10

20

30

40

50



そして、携帯機 3 は、このリクエスト信号を受信すると、前記 ID コード信号を送信する（ステップ S 28）。

セキュリティ制御装置 10 は、携帯機 3 からの ID コード信号を受信すると、該 ID コード信号に含まれる ID コードをメモリ 13 a に記録する（ステップ S 29）。すなわち、セキュリティ制御装置 10 は、取得した携帯機 3 の ID コードを自身に登録する。次いで、セキュリティ制御装置 10 は、携帯機管理装置 30 に前記登録信号を送信する（ステップ S 30）。

#### 【0081】

すなわち、ステップ S 27～S 30 においては、前記第 1 実施形態におけるステップ S 3～S 6（図 2 参照）と同等の通信が行われる。

携帯機管理装置 30 は、セキュリティ制御装置 10 からの登録信号を受信すると、該登録信号に含まれる ID コードを、車両情報と対応する ID コードの記録領域の空き領域に記録する（ステップ S 31）。また、携帯機管理装置 30 は、前記登録完了信号をセキュリティ制御装置 10 に送信する（ステップ S 32）。このため、携帯機管理装置 30 は、記録した ID コードに基づき、車両 2 に対応する携帯機 3 の管理が可能となる。

#### 【0082】

セキュリティ制御装置 10 は、携帯機管理装置 30 からの登録完了信号を受信すると、車両 2 の室内に設けられた図示しないインジケータに登録完了の旨を示す表示を行ったり、図示しないスピーカなどから該登録完了の旨を示す音響報知を行ったりする（ステップ S 33）。このため、ユーザは、携帯機 3 の登録が完了したことを確実に認識可能となる。

#### 【0083】

このように、本実施形態においてセキュリティ制御装置 10 は、ID 登録モードに切り換わった際には、まず携帯機管理装置 30 との通信を行う。その結果、セキュリティ制御装置 10 は、携帯機管理装置 30 によって ID コードの登録が許可された場合に、携帯機 3 との通信を行い、携帯機 3 の ID コードをメモリ 13 a に記録（登録）する。そして、セキュリティ制御装置 10 は、再び携帯機管理装置 30 との通信を行い、登録した ID コードを携帯機管理装置 30 によって管理する。このため、セキュリティ制御装置 10 に携帯機 3 の ID コードを登録する際には、携帯機管理装置 30 による許可が必要となり、該携帯機 3 の不正登録がより確実に防止される。

#### 【0084】

したがって、本実施形態によれば、前記第 1 実施形態における（1）、（3）及び（4）の効果に加え、以下の効果を得ることができる。

（5）ID 登録制御時にあっては、登録対象となる ID コードの登録が妥当か否かの判断が携帯機管理装置 30 によって行われ、該 ID コードの登録が妥当であると判断されないと、セキュリティ制御装置 10 は、該 ID コードをメモリ 13 a に記録することができない。すなわち、セキュリティ制御装置 10 は、携帯機管理装置 30 による許可がない限り、携帯機 3 の ID コードをメモリ 13 a に新たに記録することができない。このため、ID コードの不正な登録をより一層防止することができ、セキュリティ機器のセキュリティレベルをさらに向上させることができる。

#### 【0085】

（6）セキュリティ制御装置 10 は、セキュリティ制御モードから ID 登録モードに切り換わると、まず携帯機管理装置 30 に対して ID コードの登録の許可を求めるようになっている。そして、セキュリティ制御装置 10 は、携帯機管理装置 30 から該登録の許可がなされたことを条件として携帯機 3 との通信を行い、携帯機 3 の ID コードを登録するようになっている。これに対し、セキュリティ制御装置 10 は、携帯機管理装置 30 から該登録の許可がなされない場合には、携帯機 3 との通信自体を行わないようになっている。すなわち、ID コードの登録が不能な場合には、携帯機 3 とセキュリティ制御装置 10 との通信が行われない。このため、携帯機 3 とセキュリティ制御装置 10 との無駄な通信を防止することができ、携帯機 3 及びセキュリティ制御装置 10 の電力消費量を低減する

ことができる。

【0086】

なお、この第2実施形態は以下のように変更してもよい。

・ 前記第2実施形態の車両用セキュリティ制御システム1におけるID登録モードでの通信制御(ID登録制御)では、セキュリティ制御装置10は、セキュリティ制御モードからID登録モードに切り換わると、まず携帯機管理装置30に対してIDコードの登録の許可を求めるようになっている。そして、セキュリティ制御装置10は、携帯機管理装置30から該登録の許可がなされたことを条件として携帯機3との通信を行い、携帯機3のIDコードを登録するようになっている。しかし、該ID登録制御は、こうした通信態様に限らず、図4に示すような通信態様に変更されてもよい。以下、その変更態様を、図4を用いて説明する。なお、この変更態様において、セキュリティ制御装置10の車両制御部13から出力される登録許可要求信号には、前記車両情報と、登録対象となる携帯機3のIDコードとが含まれるようになっている。

10

【0087】

まず、セキュリティ制御装置10のモードスイッチ21がユーザによって操作されると(ステップS41)、セキュリティ制御装置10はセキュリティ制御モードからID登録モードに切り換わる(ステップS42)。ID登録モードに切り換わるとセキュリティ制御装置10は、車両2の室内に前記リクエスト信号を送信する(ステップS43)。

【0088】

そして、携帯機3は、このリクエスト信号を受信すると、前記IDコード信号を送信する(ステップS44)。

20

セキュリティ制御装置10は、携帯機3からのIDコード信号を受信すると、該IDコード信号に含まれるIDコードをRAMやバッファなどに一時記憶(仮登録)する(ステップS45)。次いで、セキュリティ制御装置10は、該一時記憶したIDコードと、前記車両情報とを含む登録許可要求信号を携帯機管理装置30に送信する(ステップS46)。

【0089】

携帯機管理装置30は、該登録許可要求信号を受信すると、該登録許可要求信号に含まれる車両情報に基づき、対応するセキュリティ制御装置10へのIDコードの登録が許可状態であるか否かの判断(認証)を行う(ステップS47)。また、携帯機管理装置30は、メモリ32aにおけるIDコードの記録領域を割り出し、該記録領域に新たにIDコードを記録可能であるか否かを判断する(同ステップS47)。すなわち、ここで携帯機管理装置30は、前記第2実施形態におけるステップS24と同様の処理を行う。その結果、対応する登録認否情報が登録認可コードであり、且つメモリ32aにおいて車両情報と対応するIDコードの記憶領域に空き領域が存在する場合、携帯機管理装置30は、IDコードの登録が妥当である(認証OK)と判断する。そして、携帯機管理装置30は、登録許可要求信号に含まれるIDコード(取得したIDコード)をメモリ32aの該空き領域に記録する(ステップS48)。その後、携帯機管理装置30は、許可コードを含む応答信号をセキュリティ制御装置10に送信する(ステップS49)。

30

【0090】

これに対し、携帯機管理装置30は、車両情報に対応する登録認否情報が登録不認可コードである場合や、対応するIDコードの記録領域にIDコードを登録可能な領域が存在しない場合には、IDコードの登録が妥当ではない(認証NG)と判断し、許可コードを含む応答信号をセキュリティ制御装置10に送信しない。また、この場合、携帯機管理装置30は、異常報知信号を携帯電話4に送信する(ステップS50)。このため、前記第2実施形態と同様に、携帯機3のIDコードがセキュリティ制御装置10に登録される以前に、ユーザに対して異常報知がなされる。よって、IDコードの不正な登録を未然に防ぐことが可能となる。

40

【0091】

ところで、携帯機管理装置30から許可コードを含む応答信号が送信された場合、セキ

50

セキュリティ制御装置 10 によって該応答信号が受信されると、セキュリティ制御装置 10 は、前記一時記憶した ID コードを、メモリ 13a に記録（本登録）する（ステップ S51）。そして、セキュリティ制御装置 10 は、車両 2 の室内に設けられた図示しないインジケータに登録完了の旨を示す表示を行ったり、図示しないスピーカなどから該登録完了の旨を示す音響報知を行ったりする（ステップ S52）。このため、ユーザは、携帯機 3 の登録が完了したことを確実に認識可能となる。

#### 【0092】

このように、本変更態様においてセキュリティ制御装置 10 は、ID 登録モードに切り換わった際には、まず携帯機管理装置 30 との通信を行う。その結果、セキュリティ制御装置 10 は、携帯機管理装置 30 によって ID コードの登録が許可された場合に、携帯機 3 との通信を行い、携帯機 3 の ID コードをメモリ 13a に記録（本登録）する。そして、セキュリティ制御装置 10 は、再び携帯機管理装置 30 との通信を行い、登録した ID コードを携帯機管理装置 30 によって管理する。このため、セキュリティ制御装置 10 に携帯機 3 の ID コードを登録する際には、携帯機管理装置 30 による許可が必要となり、該携帯機 3 の不正登録がより確実に防止される。

10

#### 【0093】

また、登録許可要求信号には取得した携帯機 3 の ID コードが含まれ、該登録許可要求信号が携帯機管理装置 30 によって受信されるとともに認証 OK と判断されると、その時点で該 ID コードがメモリ 32a に記録される。このため、セキュリティ制御装置 10 と携帯機管理装置 30 との間では、前記第 2 実施形態のような 2 回の通信が必要なく、1 回の通信だけで済む。

20

#### 【0094】

よって、このように変更すれば、前記（5）の効果に加えて、ID 登録制御時における車両用セキュリティ制御システム 1 の通信態様を、第 2 実施形態よりも簡素化することができる。

#### 【0095】

##### （第 3 実施形態）

次に、本発明を具体化した第 3 実施形態を図 1 及び図 5 に基づいて説明する。

本実施形態は、前記第 1 実施形態または前記第 2 実施形態における車両用セキュリティ制御システム 1 の制御態様に加え、セキュリティ解除制限制御を行うようになっている。すなわち、本実施形態において車両用セキュリティ制御システム 1 は、前記第 1 実施形態または前記第 2 実施形態で示した ID 登録制御と、該セキュリティ解除制限制御とを併せ行うようになっている。そこで、以下、本実施形態の車両用セキュリティ制御システム 1 によって行われるセキュリティ解除制限制御について詳細に説明する。

30

#### 【0096】

本実施形態において携帯電話 4 は、ユーザによって制限操作が行われると、制限要求信号を携帯機管理装置 30 に送信する（図 1 参照）。携帯電話 4 は、例えばユーザによって設定可能な機能制限用暗証番号がテンキーから入力された際に制限操作が行われたと判断し、機能制限用暗証コードを含む制限要求信号を、携帯機管理装置 30 に送信する。また、機能制限用暗証番号とともに携帯機 3 を指定する携帯機指定番号がテンキーから入力された場合には、携帯電話 4 は、機能制限用暗証コードと携帯機指定コードとを含む制限要求信号を、携帯機管理装置 30 に送信する。ここで、機能制限用暗証コードとは、機能制限用暗証番号をバイナリー変換したものに相当する。また、携帯機指定番号とは、前記携帯機管理装置 30 のメモリ 32a に記録された ID コードの登録番号を示すものであり、携帯機指定コードとは、該携帯機指定番号をバイナリー変換したものに相当する。

40

#### 【0097】

そして、携帯機管理装置 30 は、携帯電話 4 からの制限要求信号を受信すると、機能制限信号をセキュリティ制御装置 10 に送信する制限指令制御を行う。

詳しくは、携帯機管理装置 30 は、携帯機器用通信部 33 によって制限要求信号を受信する。すなわち、携帯機器用通信部 33 は、制限要求信号を受信する受信手段として機能

50

する。このため、該制限要求信号は、管理制御部 32 に入力される。管理制御部 32 は、制限要求信号が入力されると、メモリ 32a に既に記録されている機能制限用暗証コードから、該制限要求信号に含まれる機能制限用暗証コードと対応する機能制限用暗証コードの有無を判断する（暗証コード有無判断）。

#### 【0098】

なお、機能制限用暗証コードは、車両登録制御時にメモリ 32a に記録される。該車両登録制御は、車両 2 を携帯機管理装置 30 の管理対象として設定するべく、車両 2 の車両情報を携帯機管理装置 30 に登録する制御であり、前記第 1 実施形態及び第 2 実施形態においても同様に行われる。そして、本実施形態において機能制限用暗証コードは、この車両登録制御時に、セキュリティ制御装置 10 から携帯機管理装置 30 に車両情報とともに送信され、該車両情報と対応付けをした状態でメモリ 32a に記録されるようになっている。また、携帯機管理装置 30 は、こうした車両登録制御により車両情報や機能制限用暗証コードをメモリ 32a に記録すると、車両登録が完了した旨を示す車両登録完了信号をセキュリティ制御装置 10 に送信する。

#### 【0099】

前記暗証コード有無判断の結果、制限要求信号に含まれる機能制限用暗証コードと対応する機能制限用暗証コードがメモリ 32a に存在する場合、管理制御部 32 は、該機能制限用暗証コードと対応する車両情報に基づき、制限指令制御の管理対象となる車両 2 を特定する。そして、管理制御部 32 は、その特定した車両 2 に搭載されたセキュリティ制御装置 10 に、機能制限コードを含む機能制限信号を、管理通信部 31 を介して送信する（図 1 参照）。また、制限要求信号に前記携帯機指定コードが含まれている場合、管理制御部 32 は、メモリ 32a に車両情報と対応して記録された ID コードのうち、携帯機指定コードと一致する登録番号が対応付けされた ID コードを読み出す。そして、管理制御部 32 は、読み出した ID コードと前記機能制限コードとを含む機能制限信号を、管理通信部 31 を介して送信する。

#### 【0100】

一方、セキュリティ制御装置 10 は、携帯機管理装置 30 から送信される機能制限信号を受信すると、前述した携帯機 3 との通信に基づくドアロック駆動装置 22 やエンジン制御部 23 の駆動を制限または禁止する機能制限処理を行う。

#### 【0101】

詳しくは、セキュリティ制御装置 10 は、機能制限信号をセキュリティ通信部 14 によって受信する。このため、該機能制限信号は、車両制御部 13 に入力される。車両制御部 13 は、機能制限信号が入力されると、該機能制限信号に ID コードが含まれているか否かを判断する。その結果、機能制限信号に ID コードが含まれていない場合、車両制御部 13 は、通信可能となっている何れの携帯機 3 との通信が成立しても、ドアロック駆動装置 22 やエンジン制御部 23 の制御を制限または禁止する。すなわち、この場合、車両制御部 13 は、メモリ 13a に記録されている全ての ID コードと対応する携帯機 3 との通信が成立しても、セキュリティ機器（ドアロック駆動装置 22 やエンジン制御部 23）のセキュリティ解除を制限または禁止する。また、機能制限信号に ID コードが含まれている場合、車両制御部 13 は、該 ID コードと対応する携帯機 3 との通信が成立した場合にのみ、ドアロック駆動装置 22 やエンジン制御部 23 の制御を制限または禁止する。

#### 【0102】

なお、本実施形態において車両制御部 13 は、以下の＜a＞または＜b＞に示す機能制限処理を行うようになっており、これらのうちのどちらの処理を行うかについては、ユーザによって設定可能となっている。

#### 【0103】

＜a＞第 1 機能制限処理（セキュリティ解除禁止処理）

（a-1）機能制限信号に ID コードが含まれていない場合

この場合、車両制御部 13 は、リクエスト信号に応答して送信された携帯機 3 からの ID コード信号や携帯機 3 からの施解錠指令信号を受信すると、それら ID コード信号や施

10

20

30

40

50

解錠指令信号に含まれるIDコードがメモリ13aに記録されていたとしても、ドアロック駆動装置22やエンジン制御部23の制御を行わない。すなわち、車両制御部13は、携帯機3との通信が成立しても、ドア錠の解錠やエンジンの始動を禁止する。換言すれば、機能制限信号が入力されると車両制御部13は、ドアロック駆動装置22によるドア錠の解錠やエンジン制御部23によるエンジンの始動許可といったセキュリティ解除動作を禁止する。

#### 【0104】

(a-2) 機能制限信号にIDコードが含まれている場合

この場合、車両制御部13は、リクエスト信号に応答して送信された携帯機3からのIDコード信号や携帯機3からの施解錠指令信号を受信すると、まず、該IDコード信号や施解錠指令信号に含まれるIDコードと機能制限信号に含まれるIDコードとを比較する。その結果、車両制御部13は、それらIDコード同士が一致した場合に限り、ドアロック駆動装置22やエンジン制御部23の制御を行わない。すなわち、この場合、車両制御部13は、機能制限信号に含まれるIDコードと対応する携帯機3との通信が成立した場合にのみ、ドア錠の解錠やエンジンの始動、すなわちセキュリティ解除動作を禁止する。よって、車両制御部13は、メモリ13aに記録された他のIDコード(機能制限信号に含まれていないIDコード)を含むIDコード信号や施解錠指令信号を受信した場合には、セキュリティ解除動作を通常どおり行う。つまり、ここでは、特定の携帯機3を用いたセキュリティ解除動作のみが禁止される。

#### 【0105】

<b>第2機能制限処理(セキュリティ解除制限処理)</b>

(b-1) 機能制限信号にIDコードが含まれていない場合

この場合、車両制御部13は、車両2の室外に送信したリクエスト信号に応答して送信された携帯機3からのIDコード信号や携帯機3からの施解錠指令信号を受信すると、ドアロック駆動装置22を駆動制御してドア錠の施解錠制御を行う。しかし、車両2の室内に送信したリクエスト信号に応答して送信された携帯機3からのIDコード信号を受信した場合には、車両制御部13は、エンジン始動許可状態にはならない。このため、たとえスタートスイッチが操作されても、車両制御部13はエンジン制御部23の制御を行わない。すなわち、車両制御部13は、携帯機3との通信が成立した場合、ドア錠の施解錠を行うものの、エンジンの始動については禁止する。換言すれば、機能制限信号が入力されると車両制御部13は、セキュリティ解除動作を制限する。

#### 【0106】

(b-2) 機能制限信号にIDコードが含まれている場合

この場合においても、車両制御部13は、車両2の室外に送信したリクエスト信号に回答して送信された携帯機3からのIDコード信号や携帯機3からの施解錠指令信号を受信すると、ドアロック駆動装置22を駆動制御してドア錠の施解錠制御を行う。つまり、ここでは、車両制御部13は、機能制限信号にIDコードが含まれていないときと同様にドア錠の施解錠制御を行う。しかし、IDコードを含む機能制限信号が入力された後に、車両2の室内に送信したリクエスト信号に回答して送信された携帯機3からのIDコード信号を受信した場合には、車両制御部13は、まず該IDコード信号に含まれるIDコードが機能制限信号に含まれるIDコードとを比較する。その結果、IDコード信号に含まれるIDコードが機能制限信号に含まれるIDコードと一致した場合に限り、車両制御部13は、エンジン始動許可状態にはならない。すなわち、この場合、車両制御部13は、機能制限信号に含まれるIDコードと対応する携帯機3との通信が成立した場合には、ドア錠の施解錠を行うものの、エンジンの始動については禁止する。換言すれば、IDコードを含む機能制限信号が入力されると、車両制御部13は、該IDコードと対応する携帯機3との通信に基づくセキュリティ解除動作のみを制限する。よって、車両制御部13は、メモリ13aに記録された他のIDコード(機能制限信号に含まれていないIDコード)を含むIDコード信号や施解錠指令信号を受信した場合には、セキュリティ解除動作を通常どおり行う。つまり、ここでは、特定の携帯機3を用いたセキュリティ解除動作のみが

制限される。

【0107】

なお、車両制御部13は、制限制御を解除する旨を示す制限解除信号が入力された際に、こうした機能制限制御を解除して通常のセキュリティ制御モードに切り換わる。このため、例えば制限解除信号となる制限解除番号を携帯電話4に入力し、携帯電話4、携帯機管理装置30及びセキュリティ制御装置10間の通信を行わせ、該制限解除信号をセキュリティ制御装置10に受信させれば、通常のセキュリティ制御モードに切り換わる。

【0108】

ところで、セキュリティ制御装置10は、所定の操作が行われると、車両登録モードに切り換わるようになっている。具体的には、例えば車両2に設けられた図示しない車両登録移行スイッチが操作されると、その操作の旨を示す信号（車両登録移行信号）が車両制御部13に入力される。そして、該車両登録移行信号が入力されると、車両制御部13は車両登録モードに切り換わり、車両情報を含む車両登録信号を、セキュリティ通信部14を介して携帯機管理装置30に送信する。また、車両制御部13には、図示しない入力装置（例えばカーナビゲーションシステムなどの入力部）からの入力信号が入力可能となっている。そして、車両登録モードに切り換わった後、ユーザによって設定可能な機能制限用暗証番号が該入力装置に入力され、該機能制限用暗証番号からなる入力信号が車両制御部13に入力されると、車両制御部13は、車両情報と機能制限用暗証コードとを含む車両登録信号を、セキュリティ通信部14を介して携帯機管理装置30に送信する。このため、携帯機管理装置30のメモリ32aには、車両2の車両情報や機能制限用暗証コードが対応付けされた状態で記録される。

10

20

【0109】

また、携帯機管理装置30から送信される車両登録完了信号がセキュリティ通信部14を介して車両制御部13に入力されると、該車両制御部13は、車両2の室内に設けられた図示しないインジケータに、車両2の登録が完了した旨を示す表示を行う。

【0110】

次に、本実施形態の車両用セキュリティ制御システム1において、車両2の車両情報を携帯機管理装置30に登録して車両2を携帯機管理装置30の管理対象として設定する車両登録制御時における通信態様と、機能制限制御時における通信態様とを、図5に示すシーケンスチャートを用いて説明する。

30

【0111】

<車両登録制御時における通信態様>

同図に示すように、携帯機管理装置30への車両2の登録は、セキュリティ制御装置10と携帯機管理装置30との間の通信によって行われる。

【0112】

詳しくは、まず、セキュリティ制御装置10は、車両登録モードへの移行操作が行われると、車両登録モードに切り換わる（ステップS61）。ここで、前記入力装置から機能制限用暗証番号が入力されると（ステップS62）、セキュリティ制御装置10は、車両2の車両情報と機能制限用暗証コードとを含む車両登録信号を、携帯機管理装置30に送信する（ステップS63）。

40

【0113】

携帯機管理装置30は、セキュリティ制御装置10からの車両登録信号を受信すると、該車両登録信号に含まれる車両情報及び機能制限用暗証コードをメモリ32aに記録し、管理対象となる車両2の登録（管理車両登録）を完了する（ステップS64）。このため、セキュリティ制御装置10（車両2）は、管理対象として携帯機管理装置30に登録される。そして、携帯機管理装置30は、車両登録が完了した旨を示す車両登録完了信号を、セキュリティ制御装置10に送信する（ステップS65）。

【0114】

セキュリティ制御装置10は、携帯機管理装置30からの車両登録完了信号を受信すると、車両2の登録が完了した旨をインジケータに表示することにより、登録完了の旨を通

50

知する（ステップ S 6 6）。このため、ユーザは、該インジケータを視認することにより、車両 2 の登録が完了したことを確実に認識可能となる。

【0115】

<機能制限制御時における通信態様>

同図に示すように、機能制限制御は、セキュリティ制御装置 1 0 と、携帯機管理装置 3 0 と、携帯電話 4 との間の通信によって行われる。

【0116】

詳しくは、まず、携帯電話 4 は、前記制限操作が行われて機能制限用暗証番号が入力されると（ステップ S 7 1）、機能制限用暗証コードを含む前記制限要求信号を携帯機管理装置 3 0 に送信する（ステップ S 7 2）。ここで、携帯電話 4 は、機能制限用暗証番号ととも

10

に携帯機指定番号が入力された場合には、機能制限用暗証コードと携帯機指定コードとを含む制限要求信号を携帯機管理装置 3 0 に送信する。

【0117】

携帯機管理装置 3 0 は、制限要求信号が入力されると、該制限要求信号に含まれる機能制限用暗証コードに基づいて、対応する車両 2 を特定する（ステップ S 7 3）。そして、携帯機管理装置 3 0 は、特定した車両 2 に設けられたセキュリティ制御装置 1 0 に対して、機能制限コードを含む前記機能制限信号を送信する（ステップ S 7 4）。ここで、携帯機管理装置 3 0 は、携帯機指定コードを含む制限要求信号が入力された場合には、該携帯機指定コードと対応する ID コード及び機能制限コードを含む機能制限信号を送信する。

【0118】

20

セキュリティ制御装置 1 0 は、携帯機管理装置 3 0 から機能制限信号が入力されると、前記<a>または<b>に示した機能制限処理を行う（ステップ S 7 5）。

したがって、本実施形態によれば以下の効果を得ることができる。

【0119】

（7）ユーザが所持する携帯通信機器（携帯電話 4）から送信される制限要求信号が携帯機管理装置 3 0 によって受信されると、携帯機管理装置 3 0 からセキュリティ制御装置 1 0 に対して機能制限信号が送信される。セキュリティ制御装置 1 0 は、機能制限信号を受信したことを条件として、ドアロック駆動装置 2 2 やエンジン制御部 2 3 の制御を禁止または制限する。すなわち、セキュリティ制御装置 1 0 は、該機能制限信号の受信を条件として、セキュリティ機器によるセキュリティ解除動作を禁止または制限する。このため、ユーザが携帯機 3 を紛失したり盗難されたりした場合には、携帯電話 4 から制限要求信号を送信させることにより、セキュリティ制御装置 1 0 によるセキュリティ解除動作を禁止または制限することができる。よって、携帯機 3 の紛失・盗難時においても、該携帯機 3 によるセキュリティ解除動作を即座に禁止または制限することができ、セキュリティ機器の高いセキュリティレベルを確保することができる。

30

【0120】

（8）第三者が携帯機 3 を盗難しても、該携帯機 3 を用いたセキュリティ解除動作がユーザによって簡単に禁止または制限されてしまうため、盗難後の携帯機 3 の価値は実質的に低下する。よって、第三者は、携帯機 3 を盗難しようとする気すら沸かなくなる。つまり、第三者による携帯機 3 の盗難の意欲自体を減退させることができ、携帯機 3 の盗難防止性も向上する。

40

【0121】

（9）携帯電話 4 で制限操作を行う際に、携帯機 3 を指定する携帯機指定番号がユーザによって入力されると、セキュリティ制御装置 1 0 は、該指定された携帯機 3 との通信に基づくセキュリティ解除のみを禁止または制限する。すなわち、携帯電話 4 で制限操作を行う際に、制限すべき携帯機 3 の指定を行えば、特定の携帯機 3 によるセキュリティ解除のみを禁止または制限させることができる。このため、例えば携帯機 3 を紛失したり盗難されたりした場合、その携帯機 3 によるセキュリティ解除のみを禁止または制限することができ、他に登録されている携帯機 3 によるセキュリティ解除については通常どおり可能となる。つまり、紛失したり盗難されたりしていない携帯機 3 については、何ら制限を受

50



けることなく利用可能となる。よって、機能制限が不要な携帯機 3 によるセキュリティ解除までも禁止または制限してしまうことがなく、携帯機 3 の利便性を確保することができる。

#### 【0122】

なお、本発明の実施形態は以下のように変更してもよい。

・ 前記第 1 実施形態において、セキュリティ制御装置 10 の車両制御部 13 とセキュリティ通信部 14 との間で、互いが正常に動作しているか否かを判断するための相互認証（ペアリング）を行わせてもよい。そして、互いが正常に動作していると判断された場合、すなわち該相互認証が成立した場合にのみ、携帯機 3 の ID コードをセキュリティ制御装置 10 に登録可能としてもよい。このようにすれば、例えばセキュリティ通信部 14 が不正に取り外されたり破壊されたりした場合には両者間での相互認証が成立しなくなるため、セキュリティ制御装置 10 に登録できない。よって、ID コードの不正な登録をより確実に防止できる。

10

#### 【0123】

・ 第 3 実施形態において、携帯機 3 に GPS モジュールを設け、機能制限時には携帯機 3 の位置を携帯機管理装置 30 によって認識し、該携帯機 3 の位置を携帯機管理装置 30 から携帯電話 4 に通知するようにしてもよい。このようにすれば、紛失したり盗難されたりした携帯機 3 の所在をユーザは確実に認識することができる。

#### 【0124】

・ 第 3 実施形態では、携帯電話 4 から携帯機管理装置 30 に対して制限要求信号が送信されるようになっている。しかし、車両 2 にてユーザによる制限操作を可能とし、セキュリティ制御装置 10 から携帯機管理装置 30 に対して制限要求信号を送信可能としてもよい。すなわち、車両 2 にて制限操作を行うことにより、セキュリティ機器（ドアロック駆動装置 22 やエンジン制御部 23）の機能制限を可能としてもよい。このようにすれば、機能制限を行う際に、携帯電話 4 などの携帯通信機器が不要となる。

20

#### 【0125】

・ 第 3 実施形態において車両制御部 13 は、前記セキュリティ解除禁止処理に設定されている状態で、ID コードを含まない機能制限信号が入力された場合、セキュリティ制御モード時における送信回路 11 へのリクエスト信号の出力を禁止するように変更されてもよい。このように変更すれば、機能制限信号が車両制御部 13 に入力されると、セキュリティ制御モードにおけるセキュリティ制御装置 10 と携帯機 3 との通信が不能となる。よって、携帯機 3 と車両制御部 13 との通信が成立しなくなり、車両制御部 13 によるドアロック駆動装置 22 及びエンジン制御部 23 の制御が禁止される。したがって、携帯機 3 とセキュリティ制御装置 10 との間での無駄な通信を防止することができ、携帯機 3 及びセキュリティ制御装置 10 の電力消費量を低減させることができる。

30

#### 【0126】

・ 前記第 3 実施形態において携帯機管理装置 30 は、機能制限信号をセキュリティ制御装置 10 に送信するようになっている。しかし、携帯機管理装置 30 は、機能制限対象となる携帯機 3（機能制限用暗証コードと対応付けされた ID コードを有する携帯機 3）に対して機能制限信号を送信するようになっていてもよい。なお、この場合、携帯機管理装置 30 と通信可能に携帯機 3 を構成する。さらに、携帯機管理装置 30 からの機能制限信号を受信した際に、ID コード信号や施錠指令信号を送信不能となるように携帯機 3 を構成する。このようにしても、機能制限された携帯機 3 を用いたセキュリティ解除動作が不能となり、セキュリティ機器のセキュリティレベルをより一層向上させることができる。

40

#### 【0127】

・ 前記各実施形態では、車両 2 を携帯機管理装置 30 の管理対象として設定するための車両登録制御時に、セキュリティ制御装置 10 から携帯機管理装置 30 に車両登録信号を送信させるようになっている。しかし、こうした車両登録制御時には、セキュリティ制御装置 10 とは別に設けられた登録装置から携帯機管理装置 30 に前記車両登録信

50



号を送信可能としてもよい。例えば登録装置としてパーソナルコンピュータを用い、該パーソナルコンピュータから携帯機管理装置30に車両登録信号を送信可能としてもよい。この場合、車両情報や機能制限用暗証番号などの車両登録情報をパーソナルコンピュータに入力し、インターネットなどの通信網を介して、該車両登録情報を含む車両登録信号を携帯機管理装置30に送信させるようにする。このようにすれば、車両登録作業に必ずしもセキュリティ制御装置10（車両2）が必要ではなくなるため、該車両登録作業の利便性が向上する。また、ユーザ、ディーラー、携帯機3のメーカーなどによって設定されたパスワードを車両登録信号に付与すれば、第三者による不正な車両登録を防止することができる。

#### 【0128】

さらに、車両登録信号には、セキュリティ制御装置10に登録可能な携帯機3のIDコードが1種または複数種含まれていてもよい。この場合、携帯機管理装置30が該車両登録信号を受信した際に、その信号に含まれるIDコードを登録可能IDコードとして、車両情報と対応付けした状態でメモリ32aに記録させる。そして、セキュリティ制御装置10から送信される登録信号や登録許可要求信号を携帯機管理装置30が受信した際に、該登録信号や登録許可要求信号に含まれるIDコードがメモリ32aに既に記録されている登録可能IDコードと一致するか否かに基づいて、IDコードの登録が妥当であるか否かの判断を該携帯機管理装置30に行わせる。つまりこの場合、携帯機管理装置30は、車両登録制御時に取得した登録可能IDコードのみを、セキュリティ制御装置10に登録可能なIDコードとして認識することとなる。このようにすれば、登録可能IDコードを有しない携帯機3を第三者が不正にセキュリティ制御装置10に登録しようとしても、携帯機管理装置30により該登録が妥当ではないと判断され、携帯電話4にその旨が通知される。すなわち、登録可能IDコードとして設定されたIDコードを有する携帯機3のみが、セキュリティ制御装置10に登録可能となる。よって、第三者によるIDコードの不正な登録を抑止することができ、セキュリティ機器のセキュリティレベルをさらに向上させることができる。

10

20

#### 【0129】

なお、車両2を携帯機管理装置30に登録する作業（車両登録作業）や、携帯機3のIDコードをセキュリティ制御装置10に登録する作業（ID登録作業）は、ユーザに限らず、ディーラーや携帯機3のメーカーなど、ユーザにとって信頼できる作業業者によって行われるようになっていてもよい。

30

#### 【0130】

・ 車両用セキュリティ制御システム1は、前記第1実施形態または前記第2実施形態で示したID登録制御を行わず、前記第3実施形態で示したセキュリティ解除制限制御のみを行うようになっていてもよい。

#### 【0131】

・ 前記各実施形態において、セキュリティ制御装置10と携帯機管理装置30との間の通信は、無線通信に限らず、例えば公衆通信回線を用いた有線通信が採用されてもよい。例えば、電話のモジュージャックが接続される接続口を車両2に設け、セキュリティ制御装置10と携帯機管理装置30との通信を、電話線を用いて行うようにしてもよい。

40

#### 【0132】

・ 前記各実施形態において、携帯通信機器は、携帯電話4に限らず、例えば、ノート型のパーソナルコンピュータや、PDA（Personal Digital Assistance：携帯情報端末）や、専用の通信機器などであってもよい。

#### 【0133】

・ 前記各実施形態の車両用セキュリティ制御システム1は、携帯機3とセキュリティ制御装置10との相互通信により、携帯機3が車両2に近づくことでドア錠が自動的に解錠される機能（スマートエン트리機能）と、携帯機3が車両2の室内に進入することでエンジンの始動が許可される機能（スマートイグニッション機能）とを備えている。しかし、車両用セキュリティ制御システム1は、こうしたスマートエン트리機能やスマートイグ

50

ニッション機能を備えていなくてもよい。例えば、携帯機 3 は、トランスポンダと機械鍵とを備え、該機械鍵を車両 2 に装着した際に、セキュリティ制御装置 10 との相互通信を行うようになっていてもよい。そして、セキュリティ制御装置 10 は、該トランスポンダとの相互通信が成立した際に機械鍵の回動操作を許可するとともに、該機械鍵が回動操作されたことを条件として、ドアロック駆動装置 22 やエンジン制御部 23 を制御するようになっていてもよい。つまり、セキュリティ制御装置 10 は、携帯機 3 との相互通信に基づいてセキュリティ解除動作を行うようになっていなければならない。

#### 【0134】

また、こうした携帯機 3 とセキュリティ制御装置 10 との相互通信についても必須でなくともよい。例えば、携帯機 3 は、前記施錠指令信号のみを送信可能となっていてよく、それとともに、セキュリティ制御装置 10 は、送信回路 11 を備えず、リクエスト信号を送信しないように構成されていてもよい。つまり、セキュリティ制御装置 10 は、携帯機 3 から送信される ID コードを含む送信信号に基づいてセキュリティ解除動作を行うようになってさえいれば、必ずしも携帯機 3 との相互通信を行うようになっていない必要はない。

#### 【0135】

・ 前記各実施形態において、携帯機管理装置 30 は、管理対象となる車両 2 に設けられたセキュリティ制御装置 10 に登録可能な携帯機 3 の ID コードの数を管理するようになっている。しかし、携帯機管理装置 30 は、必ずしも該 ID コードの数を管理するようになっている必要はない。

#### 【0136】

・ 前記各実施形態において車両用セキュリティ制御システム 1 は、セキュリティ制御装置 10 さえ ID 登録モードに切り換えれば、どこでも携帯機 3 の登録が可能となっている。しかし、例えばセキュリティ制御装置 10 に GPS モジュールを接続するなどして、セキュリティ制御装置 10 が予め設定された所定の場所（例えば自宅、会社、ディーラーなど）でのみ、携帯機 3 の登録が可能となるように車両用セキュリティ制御システム 1 を変更してもよい。このようにすれば、第三者による ID コードの不正な登録をさらに防止することができ、セキュリティ機器のセキュリティレベルをさらに向上させることができる。

#### 【0137】

・ 前記各実施形態において、セキュリティ制御装置 10 を ID 登録モードに切り換えるための操作は、モードスイッチ 21 の操作に限定されない。例えば、セキュリティ制御装置 10 は、車両 2 に設けられた既存のスイッチ（例えばレバーコンビネーションスイッチなど）を、所定の態様（ユーザやディーラーによるプリセットなど、ユーザやディーラーのみが知り得る態様が望ましい）で ID 登録モードに切り換わるように変更されてもよい。このようにすれば、モードスイッチ 21 を省略することができる。また、モードスイッチ 21 の誤操作により、意図しない ID 登録モードへの切り換えを防止することができる。

#### 【0138】

・ 前記携帯機管理装置 30 は、専用の管理センターに限らず、ユーザの自宅などに配設されてもよく、この場合にはパーソナルコンピュータなどによって構成されてもよい。

・ 前記各実施形態において、携帯電話 4 は、所定の音声コマンドが音声入力された際に、登録認否情報や制限要求信号を携帯機管理装置 30 に送信するようになっていてもよい。

#### 【0139】

また、携帯電話 4 と携帯機管理装置 30 との間の通信は、携帯機管理装置 30 が配設された管理センターに駐在しているオペレータとユーザとの会話によって行われてもよい。すなわち、ユーザは、携帯電話 4 を用いて管理センターに電話をかけ、オペレータとの会話により、登録認否や制限要求を指示するようになっていてもよい。この場合、指示を受けたオペレータは、該指示に基づいて携帯機管理装置 30 を操作し、登録制限制御や機能

10

20

30

40

50

制限制御を行うこととなる。このようにすれば、登録認否情報や制限要求信号を、携帯電話 4 から携帯機管理装置 30 に送信させる必要がなくなる。

【0140】

・セキュリティ機器は、ドアロック駆動装置 22 やエンジン制御部 23 に限らず、例えば、ステアリングロック装置、シフトロック装置、タイヤロック装置などであってもよい。つまり、正常な車両 2 の走行を制限または阻害するための装置であればセキュリティ機器として適用可能である。

【0141】

・セキュリティ制御システムは、車両のセキュリティ機器を制御する車両用セキュリティ制御システム 1 に限らず、例えば建物用ドアの施解錠を制御する建物用セキュリティシステムとして具体化されてもよい。

10

【0142】

次に、特許請求の範囲に記載された技術的思想のほかに、前述した実施形態によって把握される技術的思想を以下に列挙する。

(1) 請求項 3 に記載のセキュリティ制御システムにおいて、前記携帯機管理装置は、前記 ID コードの登録が妥当ではないと判断した際に、その旨を示す異常報知信号を、ユーザが所持する携帯通信機器に通報する通報制御を行うこと。この技術的思想(1)に記載の発明によれば、ユーザは、携帯機の ID コードが不正に登録されようとした旨を、携帯通信機器を通じて確実且つ迅速に認識することができる。

【0143】

20

(2) 請求項 2～4、技術的思想(1)のいずれか 1 項に記載のセキュリティ制御システムにおいて、前記携帯機管理装置は、ユーザが所持する携帯通信機器から送信される登録認否情報に基づいて、前記登録信号に含まれる ID コードの登録が妥当か否かの判断を行うこと。この技術的思想(2)に記載の発明によれば、ID コードの登録可否をユーザによって自由に設定することができる。

【0144】

(3) 請求項 1～4、技術的思想(1)、(2)のいずれか 1 項に記載のセキュリティ制御システムにおいて、前記セキュリティ制御装置は、前記セキュリティ通信手段と前記制御手段と間で互いが正常に動作しているか否かの相互認証を行い、該相互認証が成立した場合にのみ ID コードの登録を行い、該相互認証が成立しない場合には、ID コードの登録を禁止すること。この技術的思想(3)に記載の発明によれば、例えばセキュリティ通信手段が取り外されたり破壊されたりした場合には ID コードの登録が禁止されるため、ID コードの不正な登録をより確実に防止することができる。

30

【0145】

(4) 請求項 1～4、技術的思想(1)～(3)に記載のセキュリティ制御システムにおいて、前記セキュリティ制御装置は車両用であり、前記セキュリティ機器は、ドア錠の施解錠を制御するドアロック駆動装置、エンジンの始動許可を制御するエンジン制御部のうちの少なくとも一方を含んでいること。

【0146】

(5) 請求項 12 に記載のセキュリティ制御方法において、前記 ID 登録制御時には、前記セキュリティ制御装置から前記携帯機管理装置に登録許可要求信号を送信し、該携帯機管理装置が該登録許可要求信号を受信した際に、該携帯機管理装置により、前記 ID コードの登録が妥当か否かの判断を行うとともに、その判断結果を示す応答信号を前記セキュリティ制御装置に送信し、前記 ID コードの登録が妥当である旨を含む前記応答信号を前記セキュリティ制御装置が受信したことを条件として、該 ID コードを前記記録手段に登録して ID コードの登録を完了すること。

40

【図面の簡単な説明】

【0147】

【図 1】本発明を車両用セキュリティ制御システムに具体化した第 1～第 3 実施形態の概略構成を示すブロック図。

50

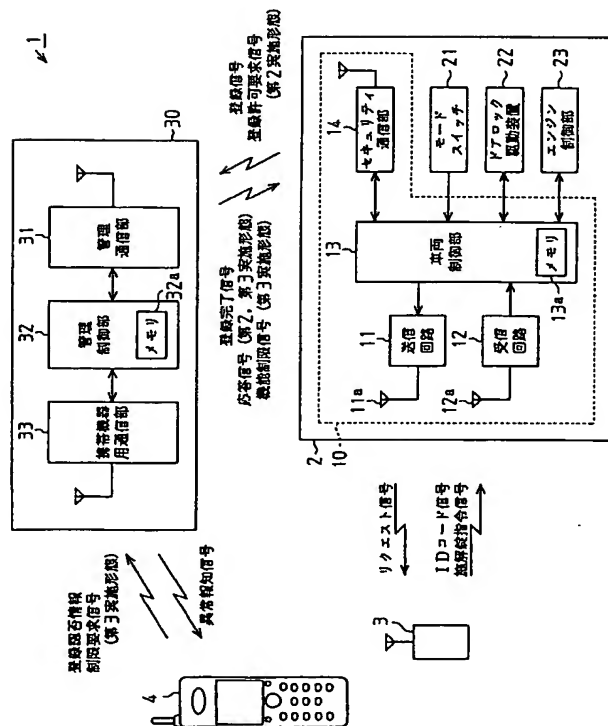
- 【図2】第1実施形態の通信態様を示すシーケンスチャート。  
 【図3】第2実施形態の通信態様を示すシーケンスチャート。  
 【図4】第2実施形態の通信態様の変更例を示すシーケンスチャート。  
 【図5】第3実施形態の通信態様を示すシーケンスチャート。  
 【符号の説明】

【0148】

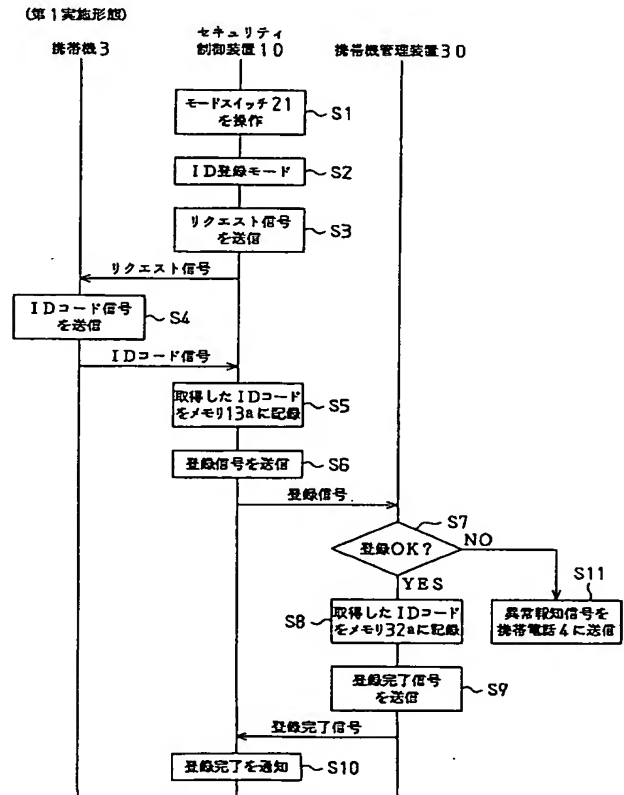
1…車両用セキュリティ制御システム、2…車両、3…携帯機、4…携帯通信機器としての携帯電話、10…セキュリティ制御装置、13…制御手段としての車両制御部、13a…記録手段としてのメモリ、14…セキュリティ通信手段としてのセキュリティ通信部、22…セキュリティ機器としてのドアロック駆動装置、23…セキュリティ機器としてのエンジン制御部、30…携帯機管理装置、31…管理通信部、32…管理手段としての管理制御部、33…携帯機器用通信手段及び受信手段としての携帯機器用通信部。

10

【図1】

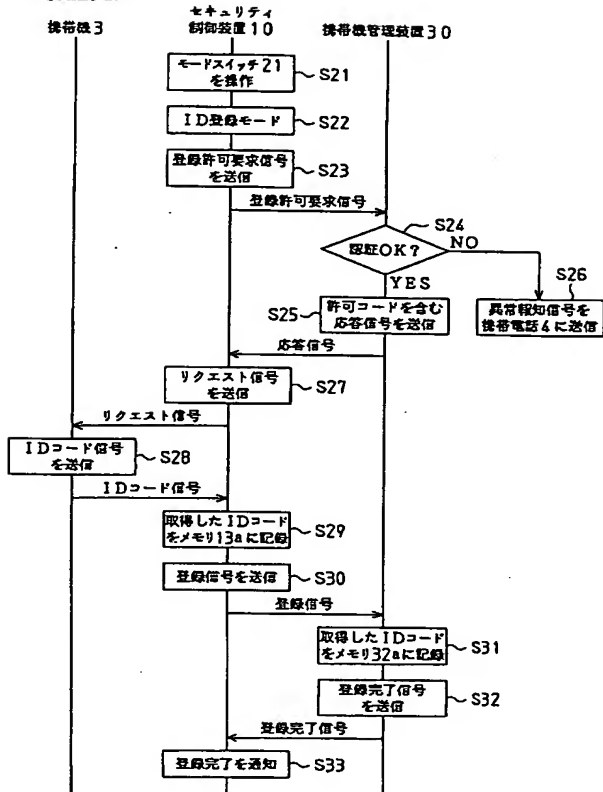


【図2】



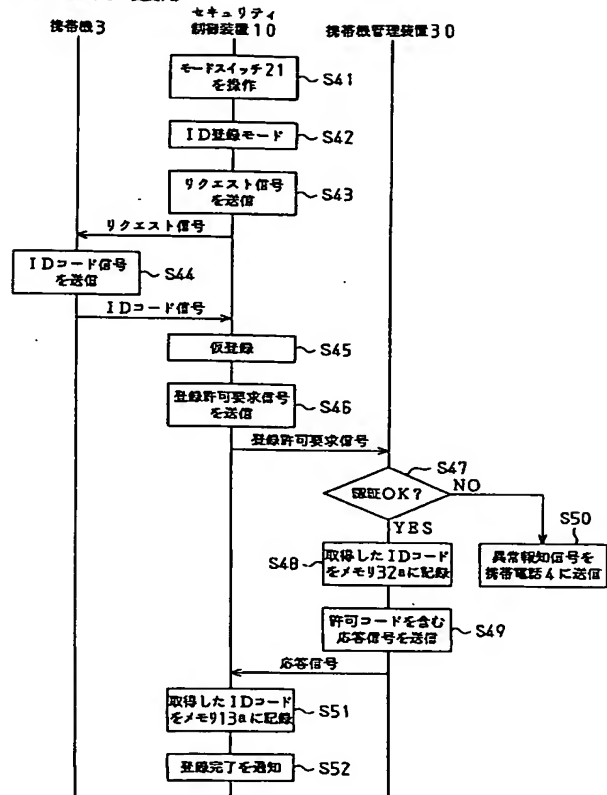
【図 3】

(第2実施形態)



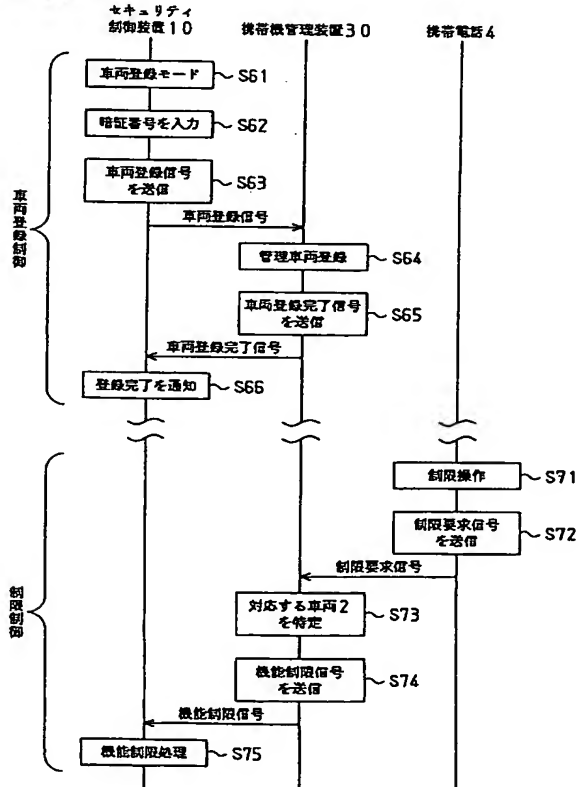
【図 4】

(第2実施形態の変更例)



【図 5】

(第3実施形態)



## フロントページの続き

(72)発明者 大滝 清和

愛知県丹羽郡大口町豊田三丁目260番地 株式会社東海理化電機製作所内

(72)発明者 山本 圭司

愛知県豊田市トヨタ町1番地 トヨタ自動車 株式会社内

(72)発明者 正村 浩一

愛知県豊田市トヨタ町1番地 トヨタ自動車 株式会社内

(72)発明者 小沢 隆夫

愛知県豊田市トヨタ町1番地 トヨタ自動車 株式会社内

(72)発明者 中根 吉英

愛知県豊田市トヨタ町1番地 トヨタ自動車 株式会社内

Fターム(参考) 2E250 AA21 BB08 BB47 BB65 CC29 FF25 FF27 FF36 GG04 GG08  
GG15 HH01 JJ00 JJ03 KK03 LL00 LL01 SS01